UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
INSTITUTO DE MATEMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA APLICADA

PRIMALIDADE E POLINÔMIOS DE CHEBYSHEV

por

Ledina Lentz Pereira

Dissertação submetida como requisito parcial
para obtenção do grau de

Mestre em Matemática Aplicada

Prof. Dr. Vilmar Trevisan
Orientador

Porto Alegre, Fevereiro de 2000.

Ao meu marido...

" O futuro pertence àqueles que acreditam na beleza de seus sonhos."

Eleonor Roosevelt

AGRADECIMENTOS

Ao Prof. Vilmar Trevisan, que acreditando em mim, aceitou o convite para ser orientador e soube com muita segurança e dedicação conduzir os trabalhos.

Agradeço aos meus filhos e meu marido que, com confiança, aceitaram minhas ausências.

À minha família, especialmente minha mãe e minha irmã Olívia, que sempre rezaram e me incentivaram dizendo que era capaz e que vale a pena lutar por nossos ideais.

Agradecendo os Professores Maria Cristina e Rudnei e a secretária do Programa Patrícia, expresso minha gratidão a todos os Professores e Funcionários desse programa de pós-graduação.

A todos os colegas de curso, em especial, Cristiane, Rosangela, Alessandra, Carolina e Evandro, pelo apoio nas horas difíceis.

A Secretaria Estadual de Educação de Santa Catarina e a Universidade do Extremo Sul Catarinense pelo apoio, me dispensando das atividades, concedendo licença.

A CAPES pela concessão de bolsa.

A Deus, por tudo...

RESUMO

Este trabalho faz uma relação entre primalidade de números inteiros e os polinômios de Chebyshev, estudando resultados recentemente descobertos. Um dos principais resultados é uma generalização do Pequeno Teorema de Fermat, que mostra a congruência, $T_n(a) \equiv a \ (mod\ n)$ para n primo, em que $T_n(x)$ é o n – ésimo polinômio de Chebyshev. A recíproca desse resultado, se verdadeira, conduziria a um teste de primalidade determinístico eficiente. Através de cálculo computacional, mostramos que para $n < 1{,}9 \times 10^4$, a recíproca é verdadeira. Além disso, os resultados dessa simulação, podem servir de base para o desenvolvimento de um algoritmo probabilístico para verificação da primalidade. Alguns testes de primalidade existentes na literatura, assim como definições e propriedades algébricas dos polinômios de Chebyshev também são apresentadas.

ABSTRACT

This work makes a relation between integer primality and Chebyshev polynomials, discussing recently found results. One of the most important results is a generalization of Fermat's little theorem. It shows that $T_n(a) \equiv a \ (mod\ n)$, for n prime, where $T_n(x)$ is the n - degree Chebyshev polynomial. The converse of this result, if true, would lead to an efficient deterministic primality test. Through a machine computation, we show that for $n < 1{,}9 \times 10^4$, the converse is true. The results of this simulation may serve to structure a probabilistic primality testing algorithm. Also, some existent primality tests, as well as definitions and algebraic properties of Chebyshev polynomials are presented.

SUMÁRIO

1- INTRODUÇÃO

Nesse capítulo apresentaremos a descrição do problema e a organização do trabalho no desenvolvimento do assunto. Também serão apresentados alguns conceitos e resultados que serão úteis para melhor compreensão do problema descrito.

1.1 – Descrição do problema e organização do trabalho

Os números primos formam a base da teoria dos números. Desde Euclides, sabemos da existência de uma infinidade de primos e que todo número inteiro é construído pelo produto de fatores primos de forma única.

Porque a quantidade de primos é infinita e a fatoração em primos é importante (especialmente em criptografia), é desejável termos métodos rápidos e fáceis para decidir se um determinado número inteiro é primo ou composto. Existem na literatura importantes pesquisas desenvolvidas, para solução desse problema. Pesquisas estas que além da classificação se desenvolveram em duas áreas: I) teste de composição – são os que testam a não primalidade de um número inteiro positivo; II) teste da primalidade – depois de passar o teste da composição, provam que o número inteiro positivo n é primo.

Sabe-se que determinar a primalidade e/ou fatoração de números inteiros é um problema muito difícil e estudado por muitos matemáticos atuais. Embora a questão da primalidade inteira versus irredutibilidade polinomial não está muito clara, é comum acreditar que seja mais fácil determinar a irredutibilidade de um polinômio de grau n do que a primalidade de um inteiro de n dígitos.

Embora polinômios de Chebyshev sejam muito estudados pelas suas propriedades analíticas (a ortogonalidade, etc), são poucos os resultados algébricos conhecidos sobre eles.

Resultados recentes [RAYES, 99] indicam que polinômios de Chebyshev podem ser usados para determinar a primalidade ou composição de números inteiros.

Uma relação entre primalidade de números inteiros e os polinômios de Chebyshev, que será aqui deduzida, mostra que $T_n(x)/x$ é irredutível se e somente se n é primo, onde $T_n(x)$ é o n-ésimo polinômio de Chebyshev. Uma conseqüência dessa relação, é considerada como uma generalização do Pequeno Teorema de Fermat: se n é primo, então $T_n(a) \equiv a \ (mod\ n)$, onde $T_n(x)$ é o n-ésimo polinômio de Chebyshev . A recíproca desse resultado, se verdadeira, como já dissemos, deverá conduzir à um teste de primalidade determinístico eficiente. Em uma tentativa para mostrar a validade da recíproca, realizamos testes computacionais que a comprovam para $n < 1{,}9 \times 10^4$. Os resultados da simulação numérica, i.e, os resultados dos cálculos computacionais feitos que poderão servir para o desenvolvimento de um algoritmo probabilístico para verificação da primalidade, serão apresentados no capítulo 6.

Sem a pretensão de apresentar uma revisão bibliográfica extensiva concernindo a testes de primalidade, apresentamos, no capítulo 2, alguns testes relevantes à nossa pesquisa. Testes esses que nos auxiliaram, sendo exemplos de testes determinísticos e também de testes probabilísticos que, em sua maioria, se fundamentam em congruência. Testes mais eficientes como de Lucas-Lehmer e Miller-Rabin, que recebem reconhecimento de estudiosos na área e também são utilizados nos computadores da atualidade são apresentados aqui, nos capítulos 3 e 4, respectivamente.

Apresentaremos no capítulo 5, definições e propriedades dos polinômios de Chebyshev como também resultados que tratam da fatoração desses polinômios, numa tentativa de ampliar os conhecimentos relativos às propriedades algébricas desses polinômios, pois a maioria da literatura existente retrata suas propriedades analíticas e a sua importante aplicação na aproximação de funções. Os principais resultados apresentados são: a completa fatoração dos polinômios de Chebyshev do primeiro e segundo tipos em fatores irredutíveis com coeficientes inteiros; Condições para a determinação da divisibilidade de um polinômio de Chebyshev por outro. Em particular, mostra-se que o resto da divisão de um polinômio de Chebyshev é, senão zero, outro polinômio de Chebyshev; A determinação de dois conjuntos infinitos de números primos p_i para os quais os polinômios de Chebyshev têm todas as raízes no corpo finito Z_{p_i}.

Terminaremos esse trabalho apresentando o algoritmo usado na simulação numérica como também os resultados obtidos na pesquisa.

A seguir apresentamos alguns resultados preliminares que serão usados no decorrer da dissertação.

1.2– Preliminares

Definição (1.1) Se a e b são inteiros dizemos que a é *congruente* a b módulo m ($m > 0$) se $m \setminus (a - b)$.

Notação: $a \equiv b \ (mod\ m)$; $a \setminus b$ *lê-se: a divide b.*

Se $m \not\setminus (a - b)$ dizemos que a é *incongruente* a b módulo m.

Notação: $a \not\equiv b \ (mod\ m)$; $a \not\setminus b$ *lê-se: a não divide b.*

Exemplo (1.1) $11 \equiv 3$ (mod 2) pois $2 \setminus (11 - 3)$. Como $5 \not\setminus 6$ e $6 = 17 - 11$ temos que $17 \not\equiv 11$ (mod 5).

Para trabalhar com inteiros congruentes é útil traduzir a congruência em igualdade. Precisaremos do seguinte teorema, para fazer isto.

Teorema (1.1) Se a e b são inteiros, então $a \equiv b \ (mod\ m)$ se, e somente se existir um inteiro k tal que $a = b + km$.

Prova. Se $a \equiv b \ (mod\ m)$, então $m \setminus (a-b)$. Isso significa que existe um inteiro k tal que $km = a - b$, isto é, $a = b + km$.

Reciprocamente, se existe um inteiro k com $a = b + km$, então $km = a-b$. Consequentemente m\(a - b) isto é, a ≡ b (mod m). □

Definição (1.2): Chama-se *sistema completo de resíduos módulo m* todo conjunto $S = \{ r_1, r_2, ..., r_m \}$ de m inteiros, tal que um inteiro qualquer a é congruente módulo m à um único elemento de S.

Exemplo (1.2) Cada um dos conjuntos:

$$\{1,2,3\}, \{0, 1, 2\}, \{-1, 0, 1\}, \{1,5,9\}$$

é um sistema completo de resíduos módulo 3.

Teorema (1.2): *Se* a, b, c e m são inteiros e $ac \equiv bc \ (mod\ m)$, *então*

$$a \equiv b \ (mod\ m/d) \text{ onde } (c,m) = d.$$

Notação: Representaremos o *mdc(a,b)* por apenas *(a,b)*

Prova. De $ac \equiv bc \ (mod\ m)$ temos $ac-bc = (a-b)c = km$. Se dividirmos os dois membros por d, teremos $(c/d)(a-b) = k\,(m/d)$. Logo $(m/d) \setminus (c/d)(a-b)$ e, como $(m/d, c/d) = 1$ temos que $(m/d) \setminus (a-b)$ o que implica $a \equiv b \ (mod\ m/d)$.□

Corolário(1.1): Se $ac \equiv bc \ (mod\ m)$ e se $(c,m) = 1$, então $a \equiv b \ (mod\ m)$.

Esta propriedade mostra que é permitido cancelar fatores de ambos os membros de uma congruência que são primos em relação ao módulo.

Corolário (1.2): Se $ac \equiv bc \ (mod\ p)$, com p primo, e se p não divide c ($p \nmid c$), então $a \equiv b \ (mod\ p)$.

Definição (1.3):*Congruência Linear em uma variável* – é toda congruência da forma

$$ax \equiv b \ (mod\ m), \qquad (1.1)$$

onde x é a incógnita e a, b e m inteiros, com $m > 0$.

Todo inteiro x_0 tal que

$$ax_0 \equiv b \ (mod\ m)$$

é uma solução da congruência linear (1.1).

Note que x_0 é uma solução da equação (1.1) se e somente se m\ ($ax_0 - b$), isto significa que existe um inteiro y_0 tal que $ax_0 - b = my_0$, de modo que o problema de achar os inteiros que satisfazem a congruência linear (1.1) reduz-se em obter todas as soluções da equação Diofantina linear $ax - my = b$.

Obtida uma solução particular x_0 da congruência linear (1.1) podemos imediatamente construir uma infinidade de outras soluções, todas mutuamente congruente módulo m. O próximo exemplo ilustra bem isto.

Exemplo (1.3): A congruência linear:

$$3x \equiv 9 \pmod{12} \qquad (1.2)$$

Como $3.3 \equiv 9 \pmod{12}$, tem-se que $x_0 = 3$ é uma solução desta congruência linear, e por conseguinte todos, os inteiros $3 + 12k$, isto é , os inteiros:

..., -33, -21, -9, 15, 27, 39, ...

também são soluções da congruência linear (1.2).

Exemplo (1.4): as soluções $x_0 = 3$ e $x_1 = -9$ da congruência linear (1.2) são congruentes módulo 12 e, portanto, não são contadas como soluções diferentes desta congruência (soluções incongruentes módulo m).

Duas soluções quaisquer da congruência (1.1), x_0 e x_1, tais que $x_0 \equiv x_1 \pmod{m}$, não são consideradas soluções distintas, isto é, o número de soluções da congruência linear (1.1) é dado pelo número de soluções mutuamente incongruentes módulo m que a satisfazem.

Antes de dar o teorema que mostra quando uma congruência linear em uma incógnita tem solução, e caso tenha, mostra exatamente quantas soluções mutuamente incongruentes ela possui, necessitamos provar um teorema que nos dá informações sobre a existência de soluções para uma equação Diofantina linear.

Teorema (1.3) Sejam a e b inteiros positivos e $d = (a, b)$. Se $d \nmid c$ então a equação $ax + by = c$ não possui nenhuma solução inteira. Se $d \mid c$ ela possui infinitas soluções e se $x = x_0$ e $y = y_0$ é uma solução particular, então todas as soluções são dadas

$$x = x_0 + (b/d)k \qquad (1.3)$$
$$y = y_0 - (a/d)k$$

onde k é um inteiro.

Prova [SANTOS, 98] Se $d \nmid c$, então a equação $ax + by = c$, não possui solução pois, como $d \mid a$ e $d \mid b$, d deveria dividir c, que é uma combinação linear de a e b. Suponhamos que $d \mid c$. Já que d pode ser escrito como combinação linear de a e b, isto é, existem inteiros n_0 e m_0, tais que

$$an_0 + b\,m_0 = d, \qquad (1.4)$$

e como $d \mid c$, existe um inteiro k tal que $c = kd$. Se multiplicarmos a equação (1.4) por k, teremos $a(n_0 k) + b(m_0 k) = kd = c$. Isto nos diz que o par (x_0, y_0) com $x_0 = n_0 k$ e $y_0 = m_0 k$ é uma solução de $ax + by = c$. É fácil a verificação de que os pares da forma (1.3) são soluções, uma vez que

$$ax + by = a\left(x_0 + (b/d)k\right) + b\left(y_0 - (a/d)k\right)$$
$$= ax_0 + \frac{ab}{d}k + by_0 - \frac{ab}{d}k$$
$$= ax_0 + by_0 = c.$$

O que acabamos de mostrar é que, conhecida uma solução particular (x_0, y_0) podemos, a partir dela, gerar infinitas soluções. Precisamos, neste momento, mostrar que toda solução da equação $ax + by = c$ é da forma $x = x_0 + (b/d)k$, $y = y_0 - (a/d)k$. Vamos supor que (x, y) seja uma solução, i.e., $ax + by = c$. Mas, como $ax_0 + by_0 = c$, obtemos, subtraindo membro a membro, que

$$ax + by - ax_0 - by_0 = a(x - x_0) + b(y - y_0) = 0,$$

o que implica $a(x - x_0) = b(y_0 - y)$. Como $d = (a, b)$ temos,

$$\left(\frac{a}{d}, \frac{b}{d}\right) = 1.$$

Portanto, dividindo – se os dois membros da última igualdade por d, teremos

$$\frac{a}{d}(x - x_0) = \frac{b}{d}(y_0 - y). \qquad (1.5)$$

Logo, $(b/d) \mid (x - x_0)$ e portanto existe um inteiro k satisfazendo $x - x_0 = k(b/d)$, ou seja, $x = x_0 + (b/d)k$. Substituindo-se este valor de x na equação (1.5) temos

$$y = y_0 - (a/d)k,$$

o que conclui a demonstração.□

Com este teorema, estamos prontos para dizer quantas soluções incongruentes (caso exista alguma) a congruência linear $ax \equiv b \ (mod\ m)$ possui.

Teorema (1.4) – Sejam a e b e m inteiros tais que $m > 0$ e $d = (a, m)$. Se $d \nmid b$, então a congruência $ax \equiv b \ (mod\ m)$ não possui nenhuma solução. Se $d \mid b$, então $ax \equiv b \ (mod\ m)$ tem exatamente d soluções incongruentes módulo m.

Prova.[ROSEN, 93] Vimos que a congruência linear $ax \equiv b \ (mod\ m)$ é equivalente a equação Diofantina linear em duas incógnitas $ax - my = b$. O inteiro x é uma solução da congruência $ax \equiv b \ (mod\ m)$ se, e somente se, existe um inteiro y tal que $ax = b + my$, ou, o que é equivalente, $ax - my = b$. Pelo teorema 1.3 sabemos que esta equação não possui nenhuma solução se $d \nmid b$ e que se $d \mid b$, ela possui infinitas soluções, dadas por

$$x = x_0 + (m/d)k \qquad \text{e} \qquad y = y_0 + (a/d)k$$

em que (x_0, y_0) é uma solução particular de $ax - my = b$. Logo a congruência linear $ax \equiv b \ (mod\ m)$ possui infinitas soluções dadas por $x = x_0 - (m/d)\,k$.

Para determinar quantas soluções incongruentes existem, encontramos a condição que descreve quando duas das soluções

$$x_1 = x_0 + (m/d)k_1 \quad \text{e} \quad x_2 = x_0 + (m/d)\,k_2$$

são congruentes módulo m. Se x_1 e x_2 são congruentes, então

$$x_0 + (m/d)k_1 \equiv x_0 + (m/d)\,k_2 (mod\ m).$$

Subtraindo x_0 de ambos os lados desta congruência, temos

$$(m/d)k_1 \equiv (m/d)\,k_2 (mod\ m).$$

Como $(m/d) \mid m$, temos $(m, m/d) = m/d$, o que nos permite o cancelamento de m/d, pelo Teorema 1.2,

$$k_1 \equiv k_2 (mod\ d).$$

Observe que m foi substituído por $d = m/(m/d)$. Isto nos mostra que soluções incongruentes serão obtidas ao tomarmos $x = x_0 - (m/d)\,k$, onde k percorre um sistema completo de resíduos módulo d, isto é, para $k = 0, 1, 2, ..., d-1$. □

Exemplo (1.5) Encontrar todas as soluções para a congruência linear

$$9x \equiv 12 \pmod{15},$$

notamos primeiro que como (9,15) = 3 e 3\12, existem exatamente três soluções incongruentes. Podemos encontrar estas soluções encontrando primeiro uma solução particular e então somando os múltiplos apropriados de 15/3 = 5.

Para encontrar uma solução particular, consideramos a equação Diofantina linear $9x - 15y = 12$. O algoritmo de Euclides mostra que

$$15 = 9.1 + 6$$
$$9 = 6.1 + 3$$
$$6 = 3.2,$$

de forma que $3 = 9 - 6.1 = 9 - (15 - 9.1) = 9.2 - 15$. Consequentemente $9.8 - 15.4 = 12$, e uma solução particular de $9x - 15y = 12$ é dado por $x_0 = 8$ e $y_0 = 4$.

Da prova do teorema 1.4 , vemos que um conjunto completo de 3 soluções incongruentes é dado por $x = x_0 \equiv 8 \pmod{15}$, $x = x_0 + 5 \equiv 13 \pmod{15}$ e $x = x_0 + 5.2 \equiv 18 \equiv 3 \pmod{15}$.

Consideramos congruência da forma especial $ax \equiv 1 \pmod{m}$. Pelo teorema (1.4) a solução desta congruência será única se, e somente se $(a,m) = 1$.

Definição (1.4): Seja a um inteiro. Chama-se *inverso de a módulo m* um inteiro a^* tal que

$$aa^* \equiv 1 \pmod{m}.$$

Exemplo (1.6) Dado que as soluções de $7x = 1 \pmod{31}$ satisfazem $x = 9 \pmod{31}$, 9, e todos os inteiros congruentes à 9 módulo 31, são inverso de 7 módulo 31. Analogamente, como $9.7 = 1 \pmod{31}$, 7 é inverso de 9 módulo 31.

Queremos saber quais inteiros são o próprio inverso módulo p, onde p é primo. Segue o teorema que nos fala quais inteiros têm esta propriedade.

Teorema (1.6). Seja p primo. O inteiro positivo a é seu próprio inverso módulo p, se e somente se $a \equiv 1 \pmod{p}$ ou $a \equiv -1 \pmod{p}$.

Prova. [SANTOS, 98]. Se a é o seu próprio inverso, então $a^2 \equiv 1 \pmod{p}$ o que significa que $p \mid (a^2 - 1)$. Mas se $p \mid (a-1)(a+1)$, sendo p primo, $p \mid (a-1)$ ou $p \mid (a+1)$, o que implica $a \equiv 1 \pmod{p}$ ou $a \equiv -1 \pmod{p}$. Reciprocamente, se $a \equiv 1 \pmod{p}$ ou $a \equiv -1 \pmod{p}$, então $p \mid (a-1)$ ou $p \mid (a+1)$. Portanto, $p \mid (a-1)(a+1)$ o que significa $a^2 \equiv 1 \pmod{p}$.□

O nome dado ao seguinte teorema se deve ao fato de que este resultado já era conhecido, na antigüidade, pelos matemáticos chineses.

Teorema (1.6) (Teorema Chinês dos Restos) Se $(a_i, m_i) = 1$, $(m_i, m_j) = 1$ para $i \neq j$ e c_i inteiro, então o sistema

$$\begin{aligned} a_1 x &\equiv c_1 \pmod{m_1} \\ a_2 x &\equiv c_2 \pmod{m_2} \\ a_3 x &\equiv c_3 \pmod{m_3} \\ &\vdots \\ a_r x &\equiv c_r \pmod{m_r} \end{aligned}$$

possui solução e a solução é única módulo $M = m_1 . m_2 . \ldots . m_r$.

Na prova do teorema (1.6) precisaremos do seguinte resultado.

Teorema (1.7) Se $a \equiv b \pmod{m_1}$, $a \equiv b \pmod{m_2}$, ..., $a \equiv b \pmod{m_k}$ onde a, b, m_1, m_2, ..., m_k são inteiros com m_i positivos, $i = 1, 2, 3, \ldots, k$, então

$$a \equiv b \pmod{[m_1, m_2, \ldots, m_k]}$$

onde $[m_1, m_2, \ldots, m_k]$ é o mínimo múltiplo comum de $m_1, m_2, \ldots, m_k$.

Prova. [SANTOS,98] Seja p_n o maior primo que aparece nas fatorações de $m_1, m_2, \ldots, m_k$. Cada m_i, $i = 1, 2, 3, \ldots, k$ pode, então, ser expresso como

$$m_i = p_1^{\alpha_{1i}} . p_2^{\alpha_{2i}} \ldots p_n^{\alpha_{ni}},$$

(alguns α_{ji} podem ser nulos). Como $m_i \mid (a-b)$, $i = 1, 2, \ldots, k$ temos que $p_j^{\alpha_{ji}} \mid (a-b)$, $i = 1, 2, \ldots, k$, $j = 1, 2, \ldots, n$. Logo, se tomarmos $\alpha_j = \max_{1 \le i \le k} \{\alpha_{ji}\}$ teremos que

$$p_1^{\alpha_1} \cdot p_2^{\alpha_2} \ldots p_n^{\alpha_n} \setminus (a-b).$$

Mas,

$$p_1^{\alpha_1} \cdot p_2^{\alpha_2} \ldots p_n^{\alpha_n} = [m_1, m_2, \ldots, m_k]$$

o que implica $a \equiv b \ (mod\ [m_1, m_2, \ldots, m_k])$. □

Estamos prontos para provar o teorema 1.6.

Prova. [SANTOS, 98] Do fato de $(a_i, m_i) = 1$, o teorema 1.4 nos diz que $a_i x \equiv c_i \ (mod\ m_i)$ possui uma única solução que denotamos por b_i. Se definirmos $y_i = m / m_i$ em que, $m = m_1 \cdot m_2 \ldots m_r$, teremos $(y_i, m_i) = 1$, uma vez que $(m_i, m_j) = 1$ para $i \neq j$. Novamente, o teorema 1.4 nos garante que cada uma das congruências $y_i x = 1 \ (mod\ m_i)$ possui uma única solução que denotamos por $\overline{y_i}$. Logo, $y_i \overline{y_i} \equiv 1 \ (mod\ m_i)$, $i = 1, 2, \ldots, r$. Afirmamos que o número x dado por

$$x = b_1 y_1 \overline{y_1} + b_2 y_2 \overline{y_2} + \ldots + b_r y_r \overline{y_r}$$

é uma solução simultânea para o nosso sistema de congruências. De fato

$$a_i x = a_i b_1 y_1 \overline{y_1} + a_i b_2 y_2 \overline{y_2} + \ldots + a_i b_i y_i \overline{y_i} + \ldots + a_i b_r y_r \overline{y_r}$$

$$\equiv a_i b_i y_i \overline{y_i} \left(\mathrm{mod}\, m_i\right) \equiv a_i b_i \equiv c_i \left(\mathrm{mod}\, m_i\right)$$

uma vez que y_i é divisível por m_i para $i \neq j$, $y_i \overline{y_i} \equiv 1 \left(\mathrm{mod}\, m_i\right)$ e b_i é solução de $a_i x \equiv c_i \ (mod\ m_i)$.

Provamos, a seguir, que esta solução é única módulo m. Se $\overline{x}$ é uma outra solução para o nosso sistema, então $a_i \overline{x} \equiv c_i \equiv a_i x \ (mod\ m_i)$ e, sendo $(a_i, m_i) = 1$ obtemos $\overline{x} \equiv x \ (mod\ m_i)$. Logo $m_i \setminus (\overline{x} - x)$, $i = 1, 2, \ldots, r$. Mas, como $(m_i, m_j) = 1$ para $i \neq j$ temos que

$$[m_1, m_2, \ldots, m_r] = m_1 \cdot m_2 \cdot \ldots \cdot m_r.$$

Portanto, pelo teorema 1.7, $m_1 \cdot m_2 \ldots m_r \setminus (\overline{x} - x)$, ou seja $\overline{x} \equiv x \ (mod\ m)$. □

Exemplo (1.7) Resolver o sistema de congruências abaixo:

$$x \equiv 1 \ (\mathrm{mod}\ 5)$$

$$x \equiv 2 \ (\mathrm{mod}\ 7)$$

$$x \equiv 3 \ (\mathrm{mod}\ 11).$$

Utilizando a notação introduzida no teorema 1.6 temos

$m_1 = 5;\ m_2 = 7;\ m_3 = 11,\ m = 5 \times 7 \times 11$

$y_1 = m/m_1 = 7 \times 11;\ y_2 = m/m_2 = 5 \times 11;\ y_3 = m/m_3 = 5 \times 7$

Determinando $\overline{y_1}$:

$$y_1 x \equiv 1 \ (mod\ m_1),\ \text{i.e.,}$$

$$7 \times 11 x \equiv 1 \ (mod\ 5),\ \text{ou,}$$

$2x \equiv 1 \ (mod\ 5)$. Logo $\overline{y_1} = 3$.

Resolvendo $y_2 x \equiv 1 \ (mod\ m_2)$ obtemos $\overline{y_2} = 6$ e $y_3 x \equiv 1 (mod\ m_3)$ obtemos $\overline{y_3} = 6$.

Como, neste caso, $b_1 = 1$, $b_2 = 2$ e $b_3 = 3$ temos que a solução do sistema módulo $5 \times 7 \times 11$ é dada por

$$x \equiv b_1 y_1 \overline{y_1} + b_2 y_2 \overline{y_2} + b_3 y_3 \overline{y_3}$$

$$\equiv 1 \times 7 \times 11 \times 3 + 2 \times 5 \times 11 \times 6 + 3 \times 5 \times 7 \times 6$$

$$\equiv 366 \ (mod\ 385)$$

A congruência $x^2 \equiv a \ (mod\ m)$, com m primo ímpar e $(a, m) = 1$, caso tenha solução, tem exatamente duas soluções incongruentes módulo m. E poderemos definir a da seguinte forma:

Definição (1.5) Sejam a e m inteiros com $(a, m) = 1$. Dizemos que a é um resíduo quadrático módulo m se a congruência $x^2 \equiv a \ (mod\ m)$ tiver solução.

Definição (1.6) Seja p primo ímpar e a inteiro não divisível por p, definimos o *Símbolo de Legendre* $\left(\frac{a}{p}\right)$ por

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & se\ a\ e'\ um\ residuo\ quadratico\ de\ p; \\ -1, & se\ não\ e'\ um\ residuo\ quadratico\ de\ p. \end{cases}$$

É conveniente definir $\left(\frac{a}{p}\right) = 0$, quando p divide a.

Segue a propriedade mais importante do símbolo de Legendre .

Se a ≡ a'(mod p), então

$$\left(\frac{a}{p}\right)=\left(\frac{a'}{p}\right).$$

Para qualquer inteiro a, a':

$$\left(\frac{aa'}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{a'}{p}\right).$$

Assim, para o cálculo do símbolo de Legendre, é suficiente calcular $\left(\frac{q}{p}\right)$, em que q = -1, 2 ou qualquer primo ímpar diferente de p.

Euler provou a seguinte congruência:

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \ (mod\ p).$$

Em particular,

$$\left(\frac{-1}{p}\right)=\begin{cases}+1 & quando \quad p \equiv 1(\mathrm{mod}\,4)\\ -1 & quando \quad p \equiv -1(\mathrm{mod}\,4)\end{cases}$$

e

$$\left(\frac{2}{p}\right)=\begin{cases}+1 & quando \quad p \equiv \pm 1(\mathrm{mod}\,8)\\ -1 & quando \quad p \equiv \pm 3(\mathrm{mod}\,8)\end{cases}.$$

O cálculo do símbolo de Legendre $\left(\frac{q}{p}\right)$, para qualquer primo ímpar q ≠ p, pode ser executado facilmente através do algoritmo rápido (necessitando apenas divisão de Euclides) por uso da lei de reciprocidade de Gauss:

$$\left(\frac{p}{q}\right)=\left(\frac{q}{p}\right)(-1)^{\frac{p-1}{2}\times\frac{q-1}{2}}.$$

Exemplo (1.8) Como a congruência $x^2 \equiv 1\ (mod\ 7)$, $x^2 \equiv 2\ (mod\ 7)$ e $x^2 \equiv 4\ (mod\ 7)$ possuem soluções temos que

$$\left(\frac{1}{7}\right)=\left(\frac{2}{7}\right)=\left(\frac{4}{7}\right)=1$$

Por outro lado,

$$\left(\frac{3}{7}\right)=\left(\frac{5}{7}\right)=\left(\frac{6}{7}\right)=-1.$$

uma vez que as congruências $x^2 \equiv 3\ (mod\ 7)$, $x^2 \equiv 5\ (mod\ 7)$ e $x^2 \equiv 6\ (mod\ 7)$ não possuem solução.

O Símbolo de Jacobi que definimos a seguir é uma generalização do Símbolo de Legendre.

Definição(1.7) Para um inteiro a relativamente primo com o inteiro ímpar $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ o Símbolo de Jacobi, denotado por $\left(\frac{a}{n}\right)$, é definido por:

$$\left(\frac{a}{n}\right)=\left(\frac{a}{p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}}\right)=\left(\frac{a}{p_1}\right)^{\alpha_1}\left(\frac{a}{p_2}\right)^{\alpha_2}\ldots\left(\frac{a}{p_k}\right)^{\alpha_k}$$

onde os símbolos à direita da última igualdade são símbolos de Legendre.

Exemplo(1.9) Calculando o símbolo de Jacobi: $\left(\frac{2}{539}\right)$ e $\left(\frac{144}{385}\right)$,

$$\left(\frac{2}{539}\right)=\left(\frac{2}{7^2.11}\right)=\left(\frac{2}{7}\right)^2.\left(\frac{2}{11}\right)=(1)^2.(-1)=-1$$

$$\left(\frac{144}{385}\right)=\left(\frac{144}{5.7.11}\right)=\left(\frac{144}{5}\right).\left(\frac{144}{7}\right).\left(\frac{144}{11}\right)$$

$$=\left(\frac{4}{5}\right).\left(\frac{4}{7}\right).\left(\frac{1}{11}\right)=\left(\frac{2}{5}\right)^2.\left(\frac{2}{7}\right)^2.\left(\frac{1}{11}\right)=1.$$

Definição(1.8): Seja $m \in N$. Seja $E(m) = \{ x \in N \mid x \leq m \text{ e } (x, m) = 1 \}$, então $\phi(m) = \#$ $E(m)$, conhecida como função de Euler.

Exemplo(1.10) Para $n = 14$, temos $\phi(n) = 6$ e para $n = 7$ temos $\phi(7) = 6$.

Observe que para n primo $\phi(n) = n-1$, *i.e,* todos os k, $1 \leq k \leq n-1$, $(n,k)=1$.

2- TESTES DE PRIMALIDADE GERAIS

Neste capítulo apresentaremos a definição de números primos, como também mostraremos que existe uma infinidade deles e a sua importância na construção de um número inteiro n > 0. Falaremos de uma forma mais geral da existência de testes para verificar se um determinado número inteiro n é primo, classificando-os em testes de primalidade determinísticos e probabilísticos, com exemplos. Mostraremos também que o teste de primalidade de Fermat, embora não se classifique em nenhum dos dois tipos de testes citados, serve de base para muitos testes de primalidade existentes na literatura, inclusive neste trabalho.

2.1 – Números primos

Definição (2.1): Um inteiro maior que 1 é chamado primo se seus fatores positivos são apenas ele mesmo e 1.

Se $n > 1$ não é primo dizemos que n é composto.

Assim, dado um número diferente de 1, duas condições poderão ser analisadas, este número será primo ou composto, nenhuma condição a mais.

Observando o conjunto dos primos, verificamos que o único número par que é primo é o 2, pois os demais números pares serão múltiplos dele (isto é, $n = 2.n/2$), deixando assim de serem primos. Isto faz o 2 um pouco incomum entre os elementos do conjunto dos primos.

Os primos são importantes na construção de qualquer inteiro positivo $n > 1$, pois sabemos , através do Teorema Fundamental da Aritmética:

Teorema (2.1): (Euclides) Todo inteiro positivo $n > 1$ pode ser representado de maneira única(a menos da ordem) como um produto de fatores primos.

Prova[SANTOS, 98]: Se n é primo não há nada a ser demonstrado. Suponhamos, pois, n composto. Seja p_1 ($p_1 > 1$) o menor dos divisores positivos de n. Afirmamos que p_1 é primo. Isto é verdade, pois caso contrário existiria p, $1 < p < p_1$ com $p \backslash n$, contradizendo a escolha de p_1. Logo, $n = p_1 n_1$. Se n_1 for primo a prova está completa. Caso contrário, tomamos p_2 como o menor fator de n_1. Pelo argumento anterior, p_2 é primo e temos que $n = p_1 p_2 n_2$. Repetindo este procedimento, obtemos uma seqüência decrescente de inteiros $n_1, n_2, ..., n_r$. Como todos eles são inteiros maiores do que 1, este processo deve terminar. Como os primos na seqüência $p_1, p_2, ..., p_k$ não são necessariamente, distintos, n terá, em geral, a forma:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}.$$

Para mostrarmos a unicidade usamos indução em n. Para $n = 2$ a afirmação é verdadeira. Assumimos, então, que ela se verifica para todos os inteiros maiores do que 1 e menores do que n. Vamos provar que ela também é verdadeira para n. Se n é primo, não há nada a provar. Vamos supor, então, que n seja composto e que tenha duas fatorações, isto é,

$$n = p_1 p_2 ... p_s = q_1 q_2 ... q_r.$$

Vamos provar que $s = r$ e que cada p_i é igual a algum q_j. Como p_1 divide o produto $q_1 q_2 ... q_r$ ele divide pelo menos um dos fatores q_j. Sem perda de generalidade podemos supor que $p_1 \backslash q_1$. Como são ambos primos, isto implica $p_1 = q_1$. Logo $n / p_1 = p_2 ... p_s = q_2 ... q_r$. Como $1 < n / p_1 < n$, a hipótese de indução nos diz que as duas fatorações são idênticas, isto é, $s = r$ e, a menos da ordem, as fatorações $p_1 p_2 ... p_s$ e $q_1 q_2 ... q_s$ são iguais. □

Considerando a utilidade dos primos, se existissem apenas um número finito deles, então a teoria dos números poderia talvez ser mais simples; porém, Euclides mostrou provando o seguinte teorema, que tal número não existe.

Teorema (2.2): (Euclides) Existe um número infinito de primos.

Prova: Assuma que exista um número finito de primos, ou seja, $p_1, p_2, ..., p_k$. Considere o inteiro $n = p_1 p_2 ... p_k + 1$. Seja p_r um primo e suponha que $p_r \mid (p_1 p_2 ... p_k + 1)$. Mas $p_r \mid p_1 p_2 ... p_k$, que implica que $p_r \mid 1$, uma contradição. Consequentemente, n é primo, também uma contradição, pois não é nenhum dos primos $p_1, p_2, ..., p_k$. Então, nossa suposição, da existência de um número finito de primos, é falsa. Isto mostra que deve haver uma infinidade de primos.□

Exemplo (2.1) O argumento de Euclides permite a criação de uma lista de primos: começamos com uma lista que consiste no único primo {2}. Segundo Euclides, calculamos n = 2 + 1 = 3. Este n é primo, assim, o adicionamos em nossa lista, {2,3}. Usando o argumento de Euclides novamente, calculamos n = 2.3 + 1 = 7, e novamente n é primo e pode ser adicionado à lista, {2, 3, 7}. Repetindo o argumento dá n = 2.3.7 + 1 = 43, outro primo! Agora nossa lista tem quatro primos, {2,3,7,43}. Mais uma vez, computamos n = 2.3.7.43 + 1 = 1807. Neste caso, n não é primo, mas fatora como n = 13.139. Adicionamos 13 para nossa lista {2,3,7,43,13}. Mais uma vez, computamos n = 2.3.7.43.13 + 1 = 23479. Este n também não é primo, mas fatora n = 53.443. Isto dá a lista {2,3,7,43,13,53} e paramos aqui. Mas, em princípio, poderíamos continuar este processo para produzir uma lista de tamanho arbitrário de primos.

Teorema (2.3) Para qualquer inteiro positivo k, existem k inteiros consecutivos todos compostos. Em outras palavras, existem "saltos" arbitrariamente grandes na seqüência de números primos.

Prova . Para demonstrarmos este resultado observamos que como $(k+1)!$ é divisível por todos os k números entre 2 e $k+1$, então a seqüência

$$(k + 1)! + 2, (k + 1)! + 3, ..., (k + 1)! + k, (k + 1)! + (k + 1)$$

é, toda ela , composta por k números consecutivos compostos. □

Depois do Teorema Fundamental de Aritmética restaram várias importantes questões na teoria dos números com respeito a primos, das quais destacamos duas:

(a) como determinar se um inteiro n é primo;
(b) encontrar a sua distribuição entre os inteiros.

Tais questões motivam os pesquisadores matemáticos, que desde a antigüidade foram criando e aperfeiçoando métodos para decidir se um determinado inteiro positivo é primo ou composto. Mas o problema de testar a primalidade de um número sempre foi um desafio, pois busca-se um algoritmo rápido, para decidir se um número inteiro positivo n é primo ou não. Infelizmente, essa não é uma questão simples, particularmente quando n é muito grande.

2.2 – Classificação dos testes de primalidade

Existem vários teoremas que podem ser usados para afirmar que um inteiro positivo n é primo, conhecidos como testes de primalidade.

Um *teste de primalidade determinístico* é um procedimento finito T, que é aplicável a qualquer número natural n e que atribui o certificado T(n) primo ou composto. Além disto, se o certificado T(n) é que n seja primo, então poderemos ter certeza disso.

Um exemplo de teste de primalidade determinístico é o método das divisões sucessivas, que é baseado no seguinte

Teorema (2.4): Se $n > 0$ é composto, então tem um fator primo p tal que $p^2 \leq n$.

Prova: Seja p o menor fator primo de n. Se n fatora em r e s, então $p \leq r$ e $p \leq s$. Consequentemente $p^2 \leq r \,.\, s = n$. □

O procedimento é o seguinte : dado um inteiro positivo n, usamos uma seqüência de divisores de n. Essa seqüência pode ser simplesmente a seqüência de divisores primos (2, 3, 5, 7,...), onde alternadamente somamos 2 e 4, depois dos três primeiros termos. A seqüência garante conter todos os fatores primos de n. É um método ingênuo, pois requer a verificação de todo primo positivo $p \leq \sqrt{n}$ para determinar se $p \mid n$. A complexidade deste método é O($\sqrt{n}$) divisões, requerendo O($\sqrt{n}$ (log n)^2)operações.

Note que se um número tem, digamos, 200 dígitos, são necessários O($\sqrt{n}$) = O(10^{100}) divisões, o que é completamente fora do alcance da tecnologia atual.

O teorema de Wilson (provado por Lagrange em 1770) também pode ser usado como um teste de primalidade determinístico:

Teorema (2.5): Um inteiro $n > 1$ é primo se, e somente se

$$(n-1)! \equiv -1 \ (mod\ n).$$

Prova. [SCHROEDER,86] Supõe n primo

$$(n-2)! = 2.3.4... (n-3).(n-2).$$

Aqui cada fator tem seu próprio inverso (*módulo n*) em algum lugar entre os outros fatores. Assim,

$$2.3.4.... (n-3).(n-2) \equiv 1 \ (mod\ n), \qquad (2.1)$$

e multiplicando (2.1) por $n-1$ temos:

$$(n-1)! \equiv n-1 \equiv -1 \ (mod\ n).$$

A recíproca é por contradição. Vamos supor que $(n-1)! \equiv -1 (mod\ n)$, isto é, $n \mid ((n-1)! + 1)$ e que n não seja primo, ou seja, $n = rs$, $1 < r < s$ e $1 < s < n$. Nestas condições $r \mid (n-1)! + 1$ e, sendo r um divisor de n, $r \mid (n-1)!$ e, portanto, r deve dividir a diferença $(n-1)! + 1 - (n-1)! = 1$, o que é absurdo, uma vez que $r > 1$. Logo, um n satisfazendo $(n-1)! \equiv -1 \ (mod\ n)$ deve ser primo. □

Este teste não é prático para n grande, porque $n-1$ multiplicações módulo n são necessárias para encontrar $(n-1)!$, requerendo $O(n(\log n)^2)$ operações. O método das divisões sucessivas será muito mais eficiente, se comparado a verificação da divisibilidade de $(n-1)! + 1$ por n grande.

Um *teste de primalidade probabilístico* é definido semelhantemente ao determinístico, mas se o certificado for "primo", então podemos apenas afirmar que existe uma probabilidade alta de que N é primo.

Um teste deste tipo foi proposto por R. Solovay e V. Strassen em 1977. Mostraram que, se N é um inteiro composto, então existe no máximo $\frac{1}{2}\phi(n)$ bases a, $1 < a < N$, $(a,N) = 1$, tais que

$$\left(\frac{a}{N}\right) \equiv a^{(N-1)/2} (mod\ N), \qquad (2.2)$$

isto significa que para valores escolhidos de a, N satisfaz a condição de um pseudoprimo de Euler na base a, i.e, para Euler todo n composto que satisfaz a congruência $a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) (\mathrm{mod}\, n)$, é um pseudoprimo, pois para n primo essa congruência sempre será verdadeira. Se um a é encontrado para o qual a congruência (2.2) não é válida, declare que N é composto. Caso contrário, declare que N é primo. De acordo com Solovay & Strassen, a probabilidade, em cada tentativa, que a congruência indicada seja satisfeita é no máximo $\frac{1}{2}\phi(n)$ bases a, i.e, no máximo 1 a cada duas $\phi(n)$ bases a, $1 < a < N$, (a, N) = 1, passarão no teste para N composto. Isso é significativo, pois se aumentarmos o número de tentativas, a probabilidade de erros diminuirá, ou seja, a probabilidade passará a ser $1/2^t$, onde t é o número de tentativas. Para um estudo mais aprofundado ver em [SOLOVAY,77]. No capítulo 4, veremos um teste que usou também essa idéia, chamado de teste de primalidade Miller-Rabin.

Um teste bem conhecido de composição é baseado no pequeno Teorema de Fermat (1640 e provado por Euler em 1736):

Teorema (2.5): Se p é primo e a é um inteiro positivo com $p \nmid a$, então

$$a^{p-1} \equiv 1 \ (mod\, p). \qquad (2.3)$$

Para provar o pequeno teorema de Fermat, necessitaremos dos seguintes lemas relativos à divisibilidade.

Lema(2.1): Sejam a, b, m e n inteiros, se $c \mid a$ e $c \mid b$, então $c \mid (ma + nb)$.

Prova. Como $c \mid a$ e $c \mid b$, existem inteiros e e f tais que $a = ce$ e $b = cf$. Consequentemente, $ma + nb = mce + ncf = c(me + nf)$. Logo, vemos que $c \mid (ma + nb)$.

Exemplo(2.2). Como $3 \mid 21$ e $3 \mid 33$, pelo teorema(2.5) 3 divide

$$5.21 - 3.33 = 105 - 99 = 6.$$

Lema (2.2). Sejam a, b, c inteiros positivos tais que $(a,b)=1$ e $a \mid bc$, então $a \mid c$.

Prova. Como $(a,b) = 1$, existem inteiros x e y tais que $ax + by = 1$. Multiplicando ambos os lados desta equação por c, temos $acx + bcy = c$. Pelo Lema 2.1, a divide $acx + bcy$, como isto é uma combinação linear de a e bc, ambos são divisíveis por a. Consequentemente $a \mid c$.

Estamos prontos para provar o teorema(2.5).

Prova: [ROSEN,93] Considere os $p-1$ inteiros $a, 2a, ..., (p-1)a$. Nenhum destes inteiros são divisíveis por p, porque se $p \mid ja$, então pelo Lema(2.2), $p \mid j$, pois $p \nmid a$, isso é impossível porque $1 \leq j \leq p-1$. Além disso, nenhum dois a dois inteiros $a, 2a, ..., (p-1)a$ são congruentes módulo p. Para ver isto, assuma que $ja \equiv ka \pmod p$ onde $1 \leq j < k \leq p-1$. Então pelo Corolário (1.2), como $p \nmid a$, temos $j \equiv k \pmod p$. Isso é impossível, pois j e k são inteiros positivos menores que $p-1$.

Dado que os inteiros $a, 2a, ..., (p-1)a$ formam um conjuntos de $p-1$ inteiros todos incongruentes a zero e nenhum dois a dois congruente módulo p, sabemos que os resíduos positivos menores de $a, 2a, ..., (p-1)a$, elevado a alguma ordem, devem ser os inteiros $1, 2, ..., p-1$. Como conseqüência, o produto dos inteiros $a, 2a, ..., (p-1)a$ é congruente módulo p ao produto dos primeiros $p-1$ inteiros positivos. Consequentemente,

$$a \cdot 2a \cdot ... (p-1)a \equiv 1.2...(p-1) \pmod p.$$

Então,

$$a^{(p-1)}(p-1)! \equiv (p-1)! \pmod p.$$

Como $((p-1)!, p) = 1$, usando o Corolário (1.2), cancelamos $(p-1)!$ Para obter

$$a^{(p-1)} \equiv 1 \pmod p. \square$$

Ilustraremos as idéias da prova com um exemplo.

Exemplo (2.3) Sejam p = 7 e a = 3. Então, $1.3 \equiv 3 \pmod 7$, $2.3 \equiv 6 \pmod 7$, $3.3 \equiv 2 \pmod 7$, $4.3 \equiv 5 \pmod 7$, $5.3 \equiv 1 \pmod 7$, e $6.3 \equiv 4 \pmod 7$. Consequentemente, $(1.3).(2.3).(3.3).(4.3).(5.3).(6.3) \equiv 3.6.2.5.1.4 \pmod 7$, assim $3^6.1.2.3.4.5.6 \equiv 3.6.2.5.1.4 \pmod 7$, logo $3^6.6! \equiv 6! \pmod 7$, e então $3^6 \equiv 1 \pmod 7$.

Ter uma congruência como o pequeno teorema de Fermat, que seja válida para todos os inteiros a, dado um primo p, é fornecida pelo seguinte resultado.

Corolário(2.1) Se p é primo, então $a^p \equiv a \ (mod\ p)$, qualquer que seja o inteiro a.

Prova: Temos que analisar dois casos, se $p \mid a$ e se $p \nmid a$. Se $p \mid a$, então $p \mid (a(a^{p-1} - 1))$ e, portanto $a^p \equiv a \ (mod\ p)$. Se $p \nmid a$, então pelo teorema 2.1 $p \mid (a^{p-1} - 1)$ e, portanto, $p \mid (a^p - a)$. Logo, em ambos os casos, $a^p \equiv a \ (mod\ p)$.□

Contudo, existem inteiros compostos N que satisfazem $a^{N-1} \equiv 1 (mod\ N)$, com $(a,N) = 1$.

Exemplo (2.4): a) $3^{90} \equiv 1$ (mod 91), porém 91 = 7.13 é composto;

b) $2^{340} \equiv 1$ (mod 341), porém 341 = 11.31 é composto.

Logo, se N é um inteiro positivo e $0 < a < N$ é tal que $a^{N-1} \not\equiv 1 \ (mod\ N)$, então N não pode ser primo. Assim, o Pequeno Teorema de Fermat será um teste de composição, já que pode ser usado para mostrar que um inteiro positivo n não é primo. Isto motiva a seguinte definição:

Definição (2.2): Se N é um inteiro composto ímpar, com $(a, N) = 1$ e se

$$a^{N-1} \equiv 1 \ (mod\ N),$$

então dizemos que N é um pseudoprimo na base a (pseudo primo de Fermat).

Dizemos que 91, dado no exemplo(2.5(a)), é um pseudoprimo na base 3.

Existem casos que para N composto, a procura de um "a" que satisfaça, $a^{N-1} \not\equiv 1 \ (mod\ N)$, com $(a,n) = 1$, é inútil. Tal N é chamado pseudoprimo forte ou um número de Carmichael (em homenagem ao matemático americano R. Carmichael, 1912).

Se houvesse um número finito de números Carmichael e se todos pudessem ser determinados, então o Pequeno Teorema de Fermat seria mais útil como um teste de composição. Mas a existência de infinitos números de Carmichael foi estabelecido por [ALFORD,92, pp. 703-722].

Características dos números de Carmichael:

Teorema (2.6): Seja n um inteiro positivo e $t > 2$, $p_1, p_2, ..., p_t$ primos distintos com $n = \prod_{i=1}^{t} p_i$. Se $(p_i - 1) \setminus (n-1)$ para todo i, $1 \leq i \leq t$, então n é um número de Carmichael.

Prova: [ANDERSON,97] Claramente n é composto. Seja a, tal que $(a,n) = 1$. Como $n = \prod_{i=1}^{t} p_i$, $(a, p_i) = 1$ para todo i. Pelo teorema de Fermat,

$$a^{p_i-1} \equiv 1 \pmod{p_i} \text{ para } 1 \leq i \leq t.$$

Seja b_i tal que $b_i \,.\, (p_i - 1) = n-1$ para cada i. Então, para cada i,

$$a^{n-1} = \left(a^{p_i-1}\right)^{b_i} \equiv 1 \pmod{p_i}$$

e consequentemente

$$a^{n-1} \equiv 1 \left(\mod \prod_{i=1}^{t} p_i \right) \square$$

Exemplo (2.5): Considere o composto n = 1105 = 5.13.17. Suponha que (a, 1105) = 1. Claramente, (a, 5) = (a, 13) = (a,17) = 1. Do Pequeno Teorema de Fermat obtemos, n-1 = 1104 = $3.2^4.23$,

$$a^4 \equiv 1 \pmod 5 \text{ e } a^{1104} = (a^4)^{256} \equiv 1 \pmod 5$$

$$a^{12} \equiv 1 \pmod{13} \text{ e } a^{1104} = (a^{12})^{92} \equiv 1 \pmod{13}$$

$$a^{16} \equiv 1 \pmod{17} \text{ e } a^{1104} = (a^{16})^{69} \equiv 1 \pmod{17}$$

Consequentemente,

$$a^{1104} \equiv 1 \pmod{5.13.17}$$

de forma que n = 1105 é um número de Carmichael.

É normalmente muito mais difícil mostrar que um determinado inteiro positivo grande n é um número de Carmichael, do que mostrar que é um pseudoprimo de Fermat.

A recíproca do Pequeno Teorema de Fermat, como foi mostrado anteriormente, não é verdadeira, isto nos leva a declarar que não poderá ser classificado como um teste determinístico, mas é considerado a base para muitos outros resultados em Teoria dos

Números e também para muitos testes de primalidades em uso nos computadores da atualidade. Porém, até o momento, não foi encontrado qualquer teste de primalidade determinístico aplicado à números arbitrários que possuem complexidade em tempo polinomial. Mas também não foi demonstrado que nenhum teste destes existe.

O próximo capítulo apresenta um teste de primalidade determinístico, aplicável à números inteiros de forma especial $n = M_q = 2^q - 1$ (com q primo), conhecidos como primos de Mersenne.

3 – Teste de primalidade de Lucas-Lehmer

É um teste de primalidade determinístico notável, especificamente projetado para números de Mersenne, dado por D.H. Lehmer em 1934, que se baseou nas idéias de E.Lucas (1878), é conhecido como teste de primalidade de Lucas-Lehmer para primos de Mersenne . Este teste é muito eficiente e é usado junto com rotinas aritméticas de multipre-cisão, para encontrar primos de Mersenne grandes. O teste se fundamenta nas seqüências de Lucas, cuja definição e propriedades daremos a seguir .

3.1 – Seqüência de Lucas

Definição (3.1): Sejam a, b e D inteiros não nulos. Considere a equação $x^2 - ax + b = 0$; seu discriminante é $D = a^2 - 4b$, e α e β são as duas raízes:

$$\begin{cases} \alpha = \dfrac{a+\sqrt{D}}{2} \\ \beta = \dfrac{a-\sqrt{D}}{2} \end{cases}$$

Assim,

$$\begin{cases} \alpha + \beta = a \\ \alpha - \beta = \sqrt{D} \\ \alpha\beta = b \end{cases}$$

Define-se as seqüências de U_k e de V_k por

$$\begin{cases} U_k(a,b) = \dfrac{\alpha^k - \beta^k}{\alpha - \beta} \\ V_k(a,b) = \alpha^k + \beta^k \end{cases}.$$

Em particular, $U_0(a,b) = 0$, $U_1(a,b) = 1$, enquanto $V_0(a,b) = 2$, $V_1(a,b) = a$. Para $k \geq 2$, temos também

$$\begin{cases} U_k(a,b) = aU_{k-1} - bU_{k-2}, \\ V_k(a,b) = aV_{k-1} - bV_{k-2}. \end{cases} \tag{3.1}$$

As seqüências

$$\begin{cases} U(a,b) = \left(U_k(a,b)\right)_{k>0} \\ V(a,b) = \left(V_k(a,b)\right)_{k>0} \end{cases}$$

são chamadas as seqüências de Lucas associadas ao par (a,b), ou apenas seqüências de Lucas.

Exemplo (3.1) Se tomamos $a = 1$ e $b = -1$, temos $U_k(a,b) = U_{k-1} + U_{k-2}$, com $U_0 = 1$; $U_1 = 1$ é a seqüência de Fibonacci.

Seguiremos apresentando apenas propriedades necessárias para provar os resultados principais das seqüências de Lucas. Não demonstraremos todas, pois o desenvolvimento requer muitos passos, todos a nível elementar. Apresentaremos também a generalização do pequeno teorema de Fermat, para seqüências de Lucas.

Primeiro, as propriedades algébricas, então as propriedades de divisibilidade. Para simplificar a notação, escreveremos apenas U_n para $U(a,b)$, V_n para $V_n(a,b)$.

Propriedades algébricas:

(P.1)
$$\begin{aligned} U_{2n} &= U_n V_n, \\ V_{2n} &= V_n^2 - 2b^n. \end{aligned}$$

Prova. (i) Mostrando que $U_{2n} = U_n V_n$:

Usando a definição $U_{2n} = \dfrac{\alpha^{2n} - \beta^{2n}}{\alpha - \beta}$. Também, usando a definição

$$U_n V_n = \left(\frac{\alpha^n - \beta^n}{\alpha - \beta}\right)\left(\alpha^n + \beta^n\right) = \frac{\alpha^{2n} - \beta^{2n}}{\alpha - \beta} = U_{2n} \ .\square$$

(ii) Provando que $V_{2n} = V_n^2 - 2b^n$:

Por definição $V_{2n} = \alpha^{2n} + \beta^{2n}$. Também

$$V_n^2 - 2b^n = \left(\alpha^n + \beta^n\right)^2 - 2(\alpha\beta)^n \ , \text{pois } b = \alpha\beta.$$

$$= \alpha^{2n} + 2\alpha^n\beta^n + \beta^{2n} - 2\alpha^n\beta^n$$

$$= \alpha^{2n} + \beta^{2n} = V_{2n} \ . \ \square$$

(P.2)
$$U_{m+n} = U_m V_n - b^n U_{m-n},$$
$$V_{m+n} = V_m V_n - b^n V_{m-n} \quad (para \quad m \geq n).$$

Prova. (i) Provando que $U_{m+n} = U_m V_n - b^n U_{m-n}$. Para $m = n$ temos

$$U_{2n} = U_n V_n - b^n \, U_0$$

Como $U_0 = 0$ temos que $U_{2n} = U_n V_n$, que por P.1, vimos que é verdade.

Para $m > n$ temos

$$U_{m+n} = \frac{\alpha^{m+n} - \beta^{m+n}}{\alpha - \beta}.$$

$$U_m V_n - b^n U_{m-n} = \left(\frac{\alpha^m - \beta^m}{\alpha - \beta}\right)\left(\alpha^n + \beta^n\right) - \left(\alpha\beta\right)^n \left(\frac{\alpha^{m-n} - \beta^{m-n}}{\alpha - \beta}\right)$$

$$= \left(\frac{\alpha^{m+n} + \alpha^m\beta^n - \alpha^n\beta^m - \beta^{m+n}}{\alpha - \beta}\right) - \left(\frac{\alpha^m\beta^n - \alpha^n\beta^m}{\alpha - \beta}\right)$$

$$= \frac{\alpha^{m+n} - \beta^{m+n}}{\alpha - \beta} = U_{m+n} .\square$$

(ii) Provando $V_{m+n} = V_m V_n - b^n V_{m-n}$. Para $m = n$, temos

$$V_{2n} = V_n V_n - b^n \, V_0.$$

Como $V_0 = 2$ temos que $V_{2n} = V_n^2 - 2b^n$, que por P.1, vimos que é verdade.

Para m > n temos

$$V_{m+n} = \alpha^{m+n} + \beta^{m+n} \ .$$

$$V_m V_n - b^n V_{m-n} = (\alpha^m + \beta^m)(\alpha^n + \beta^n) - (\alpha\beta)^n(\alpha^{m-n} + \beta^{m-n})$$
$$= \alpha^{m+n} + \alpha^m\beta^n + \beta^{m+n} + \beta^m\alpha^n - (\alpha^m\beta^n + \alpha^n\beta^m)$$
$$= \alpha^{m+n} + \beta^{m+n} = V_{m+n}. \ \square$$

(P.3) $U_{m+n} = U_m U_{n+1} - bU_{m-1}U_n,$
$2V_{m+n} = V_m V_n + DU_m U_n.$

Prova. (i) Provando que $U_{m+n} = U_m U_{n+1} - bU_{m-1}U_n$.

Temos por definição que $U_{m+n} = \dfrac{\alpha^{m+n} - \beta^{m+n}}{\alpha - \beta}$ e

$$U_m U_{n+1} - bU_{m-1}U_n = \left(\frac{\alpha^m - \beta^m}{\alpha - b}\right)\left(\frac{\alpha^{n+1} - \beta^{n+1}}{\alpha - \beta}\right) - \alpha\beta\left(\frac{\alpha^{m-1} - \beta^{m-1}}{\alpha - \beta}\right)\left(\frac{\alpha^n - \beta^n}{\alpha - \beta}\right)$$

$$= \left(\frac{\alpha^{m+n+1} - \alpha^m\beta^{n+1} - \alpha^{n+1}\beta^m + \beta^{m+n+1}}{(\alpha - \beta)^2}\right) - \alpha\beta\left(\frac{\alpha^{m+n-1} - \alpha^{m-1}\beta^n - \alpha^n\beta^{m-1} + \beta^{m+n-1}}{(\alpha - \beta)^2}\right)$$

$$= \frac{\alpha^{m+n+1} - \alpha^m\beta^{n+1} - \alpha^{n+1}\beta^m + \beta^{m+n+1} - \alpha^{m+n}\beta + \alpha^m\beta^{n+1} + \alpha^{n+1}\beta^m - \alpha\beta^{m+n}}{(\alpha - \beta)^2}$$

$$= \frac{\alpha^{m+n+1} - \alpha^{m+n}\beta + \beta^{m+n+1} - \alpha\beta^{m+n}}{(\alpha - \beta)^2}$$

$$= \frac{\alpha^{m+n}(\alpha - \beta) - \beta^{m+n}(\alpha - \beta)}{(\alpha - \beta)^2}$$

$$= \frac{(\alpha - \beta)(\alpha^{m+n} - \beta^{m+n})}{(\alpha - \beta)^2} = \frac{\alpha^{m+n} - \beta^{m+n}}{(\alpha - \beta)} = U_{m+n}.\square$$

(ii)Provando que $2V_{m+n} = V_m V_n + DU_m U_n$.

Usando a definição $2V_{m+n} = 2(\alpha^{m+n} + \beta^{m+n})$ e

$V_m V_n + DU_m U_n = (\alpha^m + \beta^m)(\alpha^n + \beta^n) + D\left(\dfrac{\alpha^m - \beta^m}{\alpha - \beta}\right)\left(\dfrac{\alpha^n - \beta^n}{\alpha - \beta}\right)$, como $D = a^2 - 4b$ te-

mos $D = (\alpha - \beta)^2$. Substituindo na equação acima temos

$$= \left(\alpha^{m+n} + \alpha^m\beta^n + \alpha^n\beta^m + \beta^{m+n}\right) + (\alpha-\beta)^2\left(\frac{\alpha^{m+n} - \alpha^m\beta^n - \alpha^n\beta^m + \beta^{m+n}}{(\alpha-\beta)^2}\right)$$

$$= \left(\alpha^{m+n} + \alpha^m\beta^n + \alpha^n\beta^m + \beta^{m+n}\right) + \left(\alpha^{m+n} - \alpha^m\beta^n - \alpha^n\beta^m + \beta^{m+n}\right)$$

$$= 2\alpha^{m+n} + 2\beta^{m+n} = 2\left(\alpha^{m+n} + \beta^{m+n}\right) = 2V_{m+n}. \square$$

(P.4)
$$\begin{aligned} DU_n &= 2V_{n+1} - aV_n, \\ V_n &= 2U_{n+1} - aU_n. \end{aligned}$$

(P.5)
$$\begin{aligned} U_n^2 &= U_{n-1}U_{n+1} + b^{n-1}, \\ V_n^2 &= DU_n^2 + 4b^n. \end{aligned}$$

(P.6)
$$2^{n-1}U_n = \binom{n}{1}a^{n-1} + \binom{n}{3}a^{n-3}D + \binom{n}{5}a^{n-5}D^2 + \ldots,$$

$$2^{n-1}V_n = a^n + \binom{n}{2}a^{n-2}D + \binom{n}{4}a^{n-4}D^2 + \ldots.$$

(P.7) Se m for ímpar e $k \geq 1$, então

$$D^{(m-1)/2}U_k^m = U_{km} - \binom{m}{1}b^k U_{k(m-2)} + \binom{m}{2}b^{2k}U_{k(m-4)} - \ldots \pm \binom{m}{(m-1)/2}b^{\frac{m-1}{2}k}U_k,$$

$$V_k^m = V_{km} + \binom{m}{1}b^k V_{k(m-2)} + \binom{m}{2}b^{2k}V_{k(m-4)} + \ldots + \binom{m}{(m-1)/2}b^{\frac{m-1}{2}k}V_k.$$

Se m for par e $k \geq 1$, então

$$D^{m/2}U_k^m = V_{km} - \binom{m}{1}b^k V_{k(m-2)} + \binom{m}{2}b^{2k}V_{k(m-4)} + \ldots + \binom{m}{m/2}b^{(m/2)k} \times 2,$$

$$V_k^m = V_{km} + \binom{m}{1}b^k V_{k(m-2)} + \binom{m}{2}b^{2k}V_{k(m-4)} + \ldots + \binom{m}{m/2}b^{(m/2)k} \times 2.$$

(P.8) $U_m = V_{m-1} + bV_{m-3} + b^2V_{m-5} + \ldots +$ *(última soma)*,

onde

$$(\textit{última soma}) = \begin{cases} \binom{m}{m/2} b^{m/2} & \textit{se } m \textit{ for par} \\ \binom{m}{(m-1)/2} b^{(m-1)/2} a & \textit{se } m \textit{ for impar.} \end{cases}$$

Propriedades relativas à divisibilidade :

$$\text{(P.9)} \quad \begin{matrix} U_n \equiv V_{n-1} (\mathrm{mod}\, b) \\ V_n \equiv a^n (\mathrm{mod}\, b) \end{matrix}$$

Prova. (i) Provando que $U_n \equiv V_{n-1} (\mathrm{mod}\, b)$.

Basta mostrar que b divide $U_n - V_{n-1}$, i.e., existe um k tal que

$$kb = U_n - V_{n-1}.$$

Usando a definição temos que,

$$U_n - V_{n-1} = \left(\frac{\alpha^n - \beta^n}{\alpha - \beta} \right) - \left(\alpha^{n-1} + \beta^{n-1} \right)$$

$$= \frac{\alpha^n - \beta^n - (\alpha - \beta)(\alpha^{n-1} + \beta^{n-1})}{\alpha - \beta}$$

$$= \frac{\alpha^n - \beta^n - (\alpha^n + \alpha\beta^{n-1} - \alpha^{n-1}\beta - \beta^n)}{\alpha - \beta}$$

$$= \frac{-\alpha\beta^{n-1} + \alpha^{n-1}\beta}{\alpha - \beta}$$

$$= \frac{\alpha\beta(\alpha^{n-2} - \beta^{n-2})}{\alpha - \beta}$$

$= \alpha\beta U_{n-2} = bk$. Considerando $k = U_{n-2}$, b divide $U_n - V_{n-1}$.□

(ii) Provando que, $V_n \equiv a^n (\mathrm{mod}\, b)$.

Mostraremos que $b \mid (V_n - a^n)$, significa dizer que, existe um k tal que $kb = V_n - a^n$.

$V_n - a^n = \alpha^n + \beta^n - a^n$, como $a = \alpha + \beta$,

$$= \alpha^n + \beta^n - (\alpha+\beta)^n,$$

$$= \alpha^n + \beta^n - \left(\binom{n}{0}\alpha^n + \binom{n}{1}\beta\alpha^{n-1} + \binom{n}{2}\beta^2\alpha^{n-2} + \ldots + \binom{n}{n-1}\beta^{n-1}\alpha + \binom{n}{n}\beta^n\right)$$

$$= \alpha^n + \beta^n - \left(\alpha^n + \binom{n}{1}\beta\alpha^{n-1} + \binom{n}{2}\beta^2\alpha^{n-2} + \ldots + \binom{n}{n-1}\beta^{n-1}\alpha + \beta^n\right)$$

$$= \alpha\beta\left(-\binom{n}{1}\alpha^{n-2} - \binom{n}{2}\beta\alpha^{n-3} - \ldots - \binom{n}{n-1}\beta^{n-2}\right),$$

sendo $k = -\left(\binom{n}{1}\alpha^{n-2} + \binom{n}{2}\beta\alpha^{n-3} + \ldots + \binom{n}{n-1}\beta^{n-2}\right)$, na equação anterior temos que: $V_n - a^n = kb$.□

(P.10) Seja p um primo ímpar, então

$$U_{kp} \equiv D^{(p-1)/2}U_k \pmod{p},$$

e, para $e \geq 1$,

$$U_{p^e} \equiv D^{\frac{p-1}{2}e} \pmod{p}.$$

Em particular,

$$U_p \equiv \left(\frac{D}{p}\right) \pmod{p}.$$

(P.11) $V_p \equiv a \pmod{p}$.

(P.12) Se n, $k \geq 1$, então U_n divide U_{kn}.

(P.13) Se b é par e a é ímpar, então U_n é par (para n ≥ 2) e V_n é par (para $n \geq 1$).

Se b é par e a é ímpar, então U_n, V_n são ímpares (para $n \geq 1$).

Se b é ímpar e a é par, então $U_n \equiv n \pmod{2}$ e V_n é par.

Se b é ímpar e a ímpar, então U_n, V_n são pares se 3 divide n, enquanto U_n, V_n são ímpares, caso contrário.

Em particular, se U_n é par, então V_n é par.

Aqui apresentamos o resultado principal, que generaliza o pequeno teorema de Fermat:

(P.14) Seja p um primo ímpar.

Se $p \mid a$ e $p \mid b$, então $p \mid U_k$ para todo $k > 1$.

Se $p \mid a$ e $p \nmid b$, então $p \mid U_k$ exatamente quando k for par.

Se $p \nmid a$, $p \mid b$, então $p \nmid U_n$ para todo $n \geq 1$.

Se $p \nmid a$, $p \nmid b$ e $p \mid D$, então $p \mid U_k$ exatamente quando $p \mid k$.

Se $p \nmid abD$, então $p \mid U_{\psi(p)}$, onde por definição $\psi(p) = p - (D/p)$, (D/p) denota o símbolo de Legendre.

Prova.[RIBENBOIM, 89] Se $p \mid a$ e $p \mid b$, por (3.1) $p \mid U_k$ para todo $k > 1$.

Se $p \mid a = U_2$, por (P.12) $p \mid U_{2k}$ para todo $k \geq 1$. Como $p \nmid b$ e $U_{2k+1} = aU_{2k} - bU_{2k-1}$, por indução, $p \nmid U_{2k+1}$.

Se $p \nmid a$ e $p \mid b$, por indução e (3.1), $p \nmid U_n$ para todo $n \geq 1$.

Se $p \nmid aD$ e $p \mid D$, por (P.6), $2^{p-1}U_p \equiv 0 \pmod{p}$ assim $p \mid U_p$. Por outro lado, se $p \nmid n$, então por (P.6) $2^{n-1}U_n \equiv na^{n-1} \not\equiv 0 \pmod{p}$, assim $p \nmid U_n$.

Finalmente o caso mais interessante: Assuma que $p \nmid abD$.

Se $(D/p) = -1$, então por (P.6)

$$2^p U_{p+1} = \binom{p+1}{1} a^p + \binom{p+1}{3} a^{p-2} D + \ldots + \binom{p+1}{p} aD^{(p-1)/2}$$

$$\equiv a + aD^{(p-1)/2} \equiv 0 \pmod{p}, \text{ assim } p \mid U_{p+1}.$$

Se $(D/p) = 1$, existe um C tal que $a^2 - 4b = D \equiv C^2 \pmod{p}$;

Consequentemente, $a^2 \not\equiv C^2 \pmod{p}$ e $p \nmid C$. Por (P.6), note que

$$\binom{p-1}{1} = -1 \pmod{p}, \binom{p-1}{3} = -1 \pmod{p}, \ldots :$$

$$2^{p-2}U_{p-1} = \binom{p-1}{1}a^{p-2} + \binom{p-1}{3}a^{p-4}D + \binom{p-1}{5}a^{p-6}D^2 + \ldots + \binom{p-1}{p-2}aD^{(p-3)/2} \equiv$$

$$\equiv -[a^{p-2} + a^{p-4}D + a^{p-6}D^2 + \ldots + aD^{(p-3)/2}] \equiv$$

$$\equiv -a\left(\frac{a^{p-1} - D^{(p-1)/2}}{a^2 - D}\right) \equiv -a\frac{a^{p-1} - C^{p-1}}{a^2 - C^2} \equiv 0 \pmod{p}.$$

Assim, $p \backslash U_{p-1}$ □

Para a seqüência especial de Lucas $U_n(a+1, a)$, o discriminante é $D = (a-1)^2$; assim se $p \nmid a(a^2 - 1)$, temos

$$\left(\frac{D}{p}\right) = 1 \quad e \quad p \backslash U_{p-1} = \frac{a^{p-1} - 1}{a - 1}.$$

Assim p\ a^{p-1} -1 (Isto é trivial se $p \backslash a^2 - 1$) – que é o pequeno teorema de Fermat.

(P.15) Se p$\nmid$ 2bD, então $V_{p-(D/p)} \equiv 2b^{\frac{1}{2}[1-(D/p)]} \pmod{p}$.

Para os próximos resultados, assumiremos que $(a, b) = 1$.

(P.16) $(U_n, b) = 1, (V_n, b) = 1$

(P.17) Assuma que $\rho(n)$ existe. Então $n \backslash U_k$ se e somente se, $\rho(n) \backslash k$.

Notação: Se $n \geq 2$ e se existe $r \geq 1$ tal que n divide U_r, denote por $\rho(n) = (n, U)$ o menor r.

(P.18) Se (n,b) = 1, então n divide $U_{\lambda_{\alpha,\beta}(n)}$; Sendo α, β as raízes de $x^2 - ax + b$.

Notação: Se $n = \prod_{p \backslash n} p^e$, define a função de Carmichael por

$$\lambda_{\alpha,\beta}(n) = mmc\{\psi_{\alpha,\beta}(p^e)\}, \text{ onde } \psi_{\alpha,\beta}(p^e) = p^{e-1}\psi_{\alpha,\beta}(p) = p^{e-1}\left(p - \left(\frac{D}{p}\right)\right), \text{ com p} \neq 2$$

e a generalização da função de Euler por

$$\psi_{\alpha,\beta}(n) = \prod_{p \backslash n} \psi_{\alpha,\beta}(p^e).$$

Na próxima seção apresentaremos o teste de Lucas – Lehmer para primos de Mersenne.

3.2 – Teste de Lucas-Lehmer para primos de Mersenne

Precisaremos dos seguintes resultados antes de conhecer o teste de Lucas - Lehmer.

Por P.13, se N é um primo ímpar, $U = (U_n)_{n\geq 0}$ é uma seqüência de Lucas com discriminante D e o símbolo de Jacobi $(D/N) = -1$, então N divide $U_{N-(D/N)} = U_{N+1}$.

Porém é conhecido que a recíproca não é verdadeira, pois existem inteiros compostos N e seqüências de Lucas $(U_n)_{n\geq 0}$ com discriminante D, tais que N divide $U_{N-(D/N)}$. ([RIBENBOIM,89], 101)

Será conveniente introduzir para todo $D > 1$ a função ψ_D, definida como segue:

seja $N = \prod_{i=1}^{s} p_i^{e_i}$,

$$\psi_D(N) = \frac{1}{2^{s-1}} \prod_{i=1}^{s} p_i^{e_i - 1}\left(p_i - \left(\frac{D}{p_i}\right)\right).$$

Começaremos com alguns resultados preparatórios:

Teorema(3.1) Se N é ímpar, $(N,D) = 1$, então $\psi_D(N) = N - (D/N)$ se e somente se, N é primo.

Prova.[RIBENBOIM,89] Se N é primo, por definição $\psi_D(N) = N - (D / N)$.

Se $N = p^e$ com p primo, $e \geq 2$, então $\psi_D(N)$ é múltiplo de p, enquanto $N - (D/N)$ não é.

Se $N = \prod_{i=1}^{s} p_i^{e_i}$, com $s \geq 2$, então

$$\psi_D(N) \leq \frac{1}{2^{s-1}} \prod_{i=1}^{s} p_i^{e_i - 1}(p_i + 1) = 2N \prod_{i=1}^{s} \frac{1}{2}\left(1 + \frac{1}{p_i}\right) \leq 2N \times \frac{2}{3} \times \frac{3}{5} \times \cdots = \frac{4N}{5} < N - 1,$$

desde que $n > 5$. □

Teorema (3.2) Se N é ímpar, $(N,D) = 1$ e $N - (D/N)$ divide $\psi_D(N)$, então N é primo.

Prova.[RIBENBOIM, 89] Assuma que N é composto. Primeiro, $N = p^e$, com p primo, $e \geq 2$; então $\psi_D(N) = p^e - p^{e-1}(D/p)$. Consequentemente,

$$p^e - p^{e-1} < p^e - 1 \leq p^e - (D/N) \leq p^e - p^{e-1}(D/p),$$

assim $(D/p) = -1$ e $p^e \pm 1$ divide $p^e + p^{e-1} < 2p^e - 2$, que é impossível.

Se N tem pelo menos dois fatores primos distintos, do teorema (3.1), temos que $\psi_D(N) < N-1 \leq N - (D/N)$, que contradiz a hipótese. Assim N deve ser primo. □

Teorema(3.3) Se N é ímpar, $U = U(a,b)$ é uma seqüência de Lucas com discriminante D e $(N, bD) = 1$, então $N \setminus U_{\psi_D(N)}$.

Prova[RIBENBOIM,89] Como $(N,b) = 1$, então por (P.18) N divide $U_{\lambda_{\alpha,\beta}(N)}$, onde α, β são as raízes de x^2-ax+ b. Se $n = \prod_{i=1}^{s} p_i^{e_i}$, então

$$\lambda_{\alpha,\beta}(N) = \text{mmc}\left\{p_i^{e_i-1}\left(p_i - \left(\frac{D}{p_i}\right)\right)\right\} = 2mmc\left\{\frac{1}{2}p^{e_i-1}\left(p_i - \left(\frac{D}{p_i}\right)\right)\right\}$$

e $\lambda_{\alpha,\beta}(N)$ divide

$$2\prod_{i=1}^{s}\frac{1}{2}p^{e_i-1}\left(p_i - \left(\frac{D}{p_i}\right)\right) = U_{\psi_D(N)}.$$

Por (P.12), N divide $U_{\psi_D(N)}$.□

Teorema (3.4) Se N é ímpar, $U = U(a,b)$ é uma seqüência de Lucas com discriminante D tal que $(D/N) = -1$ e N divide U_{N+1}, então $(N, bD) = 1$.

Prova.[RIBEMBOIM, 89] Como $(D/N) \neq 0$, então $(N,D) = 1$.

Se existe um primo p tal que $p \setminus N$ e $p \setminus b$, como $p \nmid D = a^2 - 4b$, então $p \nmid a$. Por (P.13) $p \nmid U_n$ para todo $n \geq 1$, que contradiz a hipótese. Assim $(N, bD) = 1$. □

Teorema (3.5) Seja $N > 1$ um inteiro ímpar e $N+1 = \prod_{i=1}^{s} q_i^{f_i}$. Assuma que existe um inteiro D tal que $(D/N) = -1$, e para qualquer fator primo q_i de $N+1$, exista uma seqüência de Lucas $\left(U_n^i\right)_{n\geq 0}$ com discriminante $D = a_i^2 - 4b_i$, onde $(a_i, b_i) = 1$ ou $(N, b_i) = 1$ tal que $N \setminus U_{N+1}^i$ e $N \nmid U_{(N+1)/q_i}^i$. Então N é primo.

Prova[RIBENBOIM, 89] Pelos teoremas 3.3 e 3.4, $N \setminus U_{\psi_D(N)}^i$ para todo $i = 1, ..., s$. Seja $\rho^{(i)}(N)$ o menor inteiro r tal que $N \setminus U_r^{(i)}$. Por (P.17) ou (P.15) e a hipótese, $\rho^{(i)}(N) \setminus (N+1), \rho^{(i)}(N) \nmid (N+1)/q_i$ e também $\rho^{(i)}(N) \setminus \psi_D(N)$. Consequentemente $q_i^{f_i} \setminus \rho^{(i)}(N)$ para todo $i = 1, ..., s$. Então, $(N+1) \setminus \psi_D(N)$ e pelo teorema 3.2, N é primo.□

Estamos prontos para o teste de Lucas – Lehmer.

Teorema (3.6) (Lucas-Lehmer para primos de Mersenne M_q) Seja a = 2, b = -2; considere as seqüências de Lucas associadas $(U_k)_{k\geq 0}$, $(V_k)_{k\geq 0}$, com discriminante $D = 12$. Então $N = M_q$ é primo se e somente se, $N \setminus V_{(N+1)/2}$.

Prova.[RIBENBOIM, 89] Seja N primo. Sabendo que $U_{2k} = U_k V_k$ e $V_{2k} = V_k^2 - 2b^k$, temos

$$V_{(N+1)/2}^2 = V_{N+1} + 2b^{(N+1)/2} = V_{N+1} - 4(-2)^{(N-1)/2} \equiv V_{N+1} - 4\left(\frac{-2}{N}\right) \equiv V_{N+1} + 4 \pmod N,$$

porque

$$\left(\frac{-2}{N}\right) = \left(\frac{-1}{N}\right)\left(\frac{2}{N}\right) = -1,$$

pois $N \equiv 3 \pmod 4$ e $N \equiv 7 \pmod 8$. Então é suficiente mostrar que $V_{N+1} \equiv -4 \pmod N$.

Por (P.3), $2V_{N+1} = V_N V_1 + DU_n U_1 = 2V_N + 12U_N$; Consequentemente, por (P.11) e (P.10):

$$V_{N+1} = V_N + 6U_N \equiv 2 + 6(12/N) \equiv 2 - 6 \equiv 4 \pmod N,$$

pois

$$\left(\frac{12}{N}\right)=\left(\frac{2}{N}\right)\left(\frac{2}{N}\right)\left(\frac{3}{N}\right)=-1, \text{ com } \left(\frac{3}{N}\right)=\left(\frac{N}{3}\right)(-1)^{(N-1)/2}$$

Reciprocamente, assuma que N divide $V_{(N+1)/2}$. Então N divide U_{N+1} [Por (P.1)]. Também, por (P.5)

$$V^2_{(N+1)/2} - 12U^2_{(N+1)/2} = 4(-1)^{(N+1)/2};$$

consequentemente, como $N \backslash V_{(N+1)/2}$, então $N \backslash V^2_{(N+1)/2}$. Se $N \backslash U_{(N+1)/2}$, então $N \backslash 12U^2_{(N+1)/2}$, portanto $N \backslash 4(-1)^{(N+1)/2}$ o que é absurdo. Logo, N é primo. □

Exemplo (3.1) Primeiro notamos que a seqüência de Lucas $V_k(2,-2)$ começa como segue: 2, 2, 8, 20, 56, 152, 416, 1136, 3104, 8480, 23168, 63296, 172928, 472448, 1290752, 3526400, 9634304, ...

suponha que desejamos testar a primalidade de $N = 2^7 - 1$. Calcule $V_{(N+1)/2}$ para $N = 2^7 - 1$:

$$\begin{aligned} V_{(N+1)/2} &= V_{2^7/2} \\ &= V_{64} \\ &= 861551776580078726854108774 4 \\ &\equiv 0 \ (\mathrm{mod}\ (2^7 - 1)), \end{aligned}$$

então através do Teorema 3.6, $N = 2^7 - 1$ é primo.

Com a finalidade de computação, é conveniente substituir a seqüência de Lucas $(V_k)_{k\geq 0}$ pela seqüência seguinte de Lucas-Lehmer $(L_k)_{k\geq 1}$, recursivamente definido como segue:

$$\begin{cases} L_0 = 4 \\ L_{k+1} = L_k^2 - 2. \end{cases} \tag{3.2}$$

A seqüência de Lucas-Lehmer começa com

4, 14, 194, 37634, 1416317954, 2005956546822746114,

4023861667741036022825635656102100994,...

a razão que podemos substituir a seqüência de Lucas $V_k(2, -2)$ pela seqüência de Lucas-Lehmer L_k, é baseada nas seguintes observações:

$$\begin{cases} L_0 = V_2 / 2 \\ L_{k-1} = V_{2^k} / 2^{2^{k-1}} \end{cases} \tag{3.3}$$

Exemplo (3.2) Este exemplo mostra como calcular a seqüência de Lucas - Lehmer L_k:

$$L_0 = V_2 / 4 = 8/2 = 4$$

$$L_1 = V_{2^2} / 2^{2^2-1}$$

$$= V_4 / 2^2$$

$$= 56/4 = 14$$

$$L_2 = V_{2^3} / 2^{2^3-1}$$

$$= V_8 / 2^4$$

$$= 3104/16 = 194$$

$$L_3 = V_{2^4} / 2^{2^4-1}$$

$$= V_{16} / 2^8$$

$$= 9634304/25 = 37634$$

$$L_4 = V_{2^5} / 2^{2^5-1}$$

$$= V_{32} / 2^{16}$$

$$= 92819813433344/65536 = 1416317954$$

Assim, o Teorema 3.6 pode ser reescrito como segue:

Teorema (3.7) (Teste de Lucas - Lehmer para primos de Mersenne M_n)
Seja n um primo ímpar. Então $2^n - 1$ é primo se e somente se, M_n divide L_{n-2}. Quer dizer,

$$L_{n-2} \equiv 0 \ (mod \ (2^n - 1)). \qquad (3.4)$$

Prova. [YAN, 96] Seja $L_0 = 4 = V_2 / 2$. Assuma que $L_{k-1} = V_{2^k} / 2^{2^k-1}$. Então

$$L_k = L_{k-1}^2 - 2$$

$$= \frac{V_{2^k}^2}{2^{2^k}} - 2$$

$$= \frac{V_{2^{k+1}+2^{2^k}+1}}{2^{2^k}} - 2$$

$$= \frac{V_{2^{k+1}}}{2^{2^k}}.$$

Pelo teorema 3.6 M_n é primo se e somente se, M_n divide

$$V_{(M_n+1)/2} = V_{2^{n-1}} = 2^{2^{n-2}} L_{n-2},$$

ou equivalentemente, $L_{n-2} \equiv 0\left(\mathrm{mod}\left(2^n - 1\right)\right).\square$

Exemplo (3.3) Suponha que desejamos testar a primalidade de 2^7 - 1; calculamos primeiro a seqüência de Lucas-Lehmer $\{L_k\}$ para 2^7 - 1 (k = 0, 1,..., p-2 = 5):

$L_0 = 4$; $L_1 = 14$; $L_2 = 67$; $L_3 = 42$; $L_4 = 111$; $L_5 = 0$ (mod 127).

Como $L_{p-2} = 0$ (mod $(2^p - 1)$), então 2^7 - 1 é primo.

Vários outros testes determinísticos clássicos são discutidos na literatura. Esses métodos requerem a fatoração de *n-1* (ou *n+1*). O problema é que para *n* grande nem todos os fatores primos de *n-1* (ou *n+1*) podem ser conhecidos. Métodos de primalidade nesta categoria incluem o teste de Pockliton-Lehmer.

Um teste que é aplicável para números naturais arbitrários N, sem requerer o conhecimento dos fatores de n-1 ou n+1 [RIBENBOIM,89, pp.115] e que possui a complexidade quase polinomial é o teste de primalidade determinístico elaborado por Adleman, Pomerance & Rumely(1983) conhecido como teste APR. Não o citamos neste trabalho, pois para justificar o mesmo segundo [RIBENBOIM, 89, p.107] é necessário resultados profundos da teoria de números algébricos; envolve cálculos com raízes da unidade e a lei de reciprocidade geral para o símbolo de resíduo de potência. Recentemente, Adleman et. al desenvolveram um teste de primalidade determinístico baseado na teoria de curvas elípticas. O teste foi mais tarde simplificado e melhorado por Lenstra e Cohen. Este algoritmo é $O(\ln n)^{C\ln(\ln(\ln n)))}$ é quase, mas não é, um algoritmo de tempo polinomial.

Uma melhoria adicional e imediata sobre o teste de Fermat é o teste de pseudo primalidade forte de Miller, que Rabin aproveitando as mesmas idéias transformou-o num teste de primalidade probabilístico respeitado, que apresentaremos no próximo capítulo.

4 – Teste de primalidade de Miller-Rabin

Neste capítulo apresentaremos dois testes de primalidade, primeiro o de Miller para depois o de Miller-Rabin, pois Rabin também usou o teste de Miller na criação de seu teste probabilístico para primalidade, i.e, fez um estudo probabilístico no teste de Miller para criar o teste, que chamaremos, Miller - Rabin.

4.1 – Teste de Primalidade de Miller

Em 1975, Miller propôs um teste de primalidade, que envolve a congruência usada na definição de pseudoprimo forte, cuja definição é a 4.2 abaixo.

Para compreender a definição de pseudo primo forte, precisaremos da seguinte definição:

Definição (4.1). Seja n um inteiro positivo com $n\text{-}1 = 2^s t$, para $s > 0$ e t inteiro positivo ímpar. Dizemos que n passa no teste de Miller para base b, se

$$b^t \equiv 1 (\mathrm{mod}\, n) \quad \text{ou} \quad b^{2^j t} \equiv -1 (\mathrm{mod}\, n), \text{ com } 0 \leq j \leq s\text{-}1.$$

Definição (4.2) Se n é composto e passa no teste de Miller para a base b, então dizemos que n é um pseudoprimo forte na base b.

O seguinte exemplo mostra que 2047 passa no teste de Miller para base 2.

Exemplo (4.1). Seja n = 2047 = 23.89. Então

$$2^{2046} = (2^{11})^{186} = (2048)^{186} \equiv 1 \text{ (mod 2047)},$$

isto mostra que 2047 é um pseudo primo na base 2. Como $2^{2046/2} = 2^{1023} = (2^{11})^{93} = (2048)^{93} \equiv 1$ (mod 2047), 2047 passa no teste de Miller para base 2.

O resultado seguinte mostra que se n é primo, então n passa no teste de Miller para todas as bases b, com $n \nmid b$.

Teorema (4.1). Se n é primo e b um inteiro positivo com $n \nmid b$, então n passa no teste de Miller para a base b.

Prova.[ROSEN, 93] Seja $n - 1 = 2^s t$, com $s > 0$ e t um inteiro positivo ímpar. Seja $x_k = b^{(n-1)/2^k} = b^{2^{s-k}t}$, para $k = 0, 1, 2, \ldots, s$. Como n é primo, o pequeno teorema Fermat diz que $x_0 = b^{n-1} \equiv 1 \pmod{n}$. Pelo teorema 1.6, já que $x_1^2 = \left(b^{(n-1)/2}\right)^2 = x_0 \equiv 1 (\mathrm{mod}\, n)$, $x_1 \equiv -1 \pmod{n}$ ou $x_1 \equiv 1 \pmod{n}$. Se $x_1 \equiv 1 (\mathrm{mod}\, n)$, como $x_2^2 = x_1 \equiv 1 (\mathrm{mod}\, n)$, $x_2 \equiv -1 \pmod{n}$ ou $x_2 \equiv 1 \pmod{n}$. Em geral, se encontramos que $x_0 \equiv x_1 \equiv x_2 \equiv \ldots \equiv x_k \equiv 1 \pmod{n}$, com $k < s$, então, como $x_{k+1}^2 = x_k \equiv 1 (\mathrm{mod}\, n)$, sabemos que $x_{k+1} \equiv 1 \pmod{n}$ ou $x_{k+1} \equiv -1 \pmod{n}$.

Continuando esse procedimento para $k = 1, 2, \ldots, s$, achamos $x_k \equiv 1 \pmod{n}$, para $k = 0, 1, 2, \ldots, s$, ou $x_k \equiv -1 \pmod{n}$ para algum inteiro k. Consequentemente, n passa no teste de Miller para base b. □

Se o inteiro positivo n passar no teste de Miller para base b, então $b^t \equiv 1 \pmod{n}$ ou $b^{2^j t} \equiv -1 (\mathrm{mod}\, n)$, com $0 \leq j \leq s-1$, onde $n-1 = 2^s t$ e t ímpar.

Em qualquer caso, temos $b^{n-1} \equiv 1 (\mathrm{mod}\, n)$, como $b^{n-1} = \left(b^{2^j t}\right)^{2^{s-j}}$ para $j = 0, 1, 2, \ldots, s$, assim um inteiro n que passa no teste de Miller para base b é automaticamente um pseudoprimo na base b. O teste de Miller pode ser implementado eficientemente; de fato o resultado seguinte precisa melhor.

Teorema (4.2) O teste de Miller é realizado em $O(\log_2 n)^3$ operações aritméticas.

Prova. O custo do teste de Miller é o custo da operação $a^n \bmod n$. O número de operações (multiplicação/adição) para esta operação é $O(\log n)$ [KNUTH, 98] sem levar em conta o número de dígitos. Se a e b tem k dígitos, então o produto $a.b$ pode ser efetuado $O(k^2)$ ope-

rações aritméticas. Assim, como há *O(log n)* multiplicações/divisões, cada uma delas envolvendo números com *log n* dígitos, segue o resultado. □

Existe uma conjectura famosa na teoria analítica dos números chamada a hipótese de Riemann generalizada que é uma declaração sobre a função zeta de Riemann. Uma conseqüência desta hipótese é a conjectura seguinte.

Conjectura (4.1) Para todo inteiro composto *n*, existe uma base *b*, $1< b < 2(\log_2 n)^2$, tal que *n* fracassa no teste de Miller para a base b.

Se essa conjectura é verdadeira, como muitos teoristas de números acreditam, o resultado seguinte provê um teste de primalidade rápido.

Teorema (4.3) Se a hipótese de Riemann generalizada é válida, então há um algoritmo para determinar se um inteiro positivo *n* é primo usando $O((\log_2 n)^5)$ operações.

Prova.(ROSEN,93) Seja *b* um inteiro positivo menor que *n*. Pelo teorema 4.2 executar o teste de Miller para a base *b* em *n* leva $O((\log_2 n)^3$ operações. Assuma que a hipótese de Riemann generalizada seja verdadeira. Se *n* é composto, então pela conjectura 4.1, existe uma base b com $1< b < 2(\log_2 n)^2$, tal que *n* falha no teste de Miller na base *b*. Descobrir este *b* requer menos que $O((\log_2 n)^3).O((\log_2 n)^2) = ((\log_2 n)^5)$ operações. Consequentemente, usando $O((\log_2 n)^5)$ operações podemos determinar se *n* é composto ou primo.□

4.2 – Teste de Primalidade de Rabin

O Resultado de Rabin mostra que o teste de Miller pode ser transformado em um teste de composição probabilístico. Quer dizer, o algoritmo produz e emprega *k* números aleatórios. Se o teste declara que n é composto, então sempre estará correto. Se o resultado final afirma que n é primo, então, as vezes, pode estar errado. Mas a probabilidade que um número composto seja declarado como primo erroneamente é menor que $1/2^{2k}$.

Apresentaremos o principal resultado de Rabin:

Teorema 4.4: Seja $n > 1$ um inteiro composto ímpar. Então n passa no teste de Miller no máximo para $(n-1)/4$ bases b com $1 \leq b < n$.

Precisaremos das seguintes definições e lema na prova.

Definição (4.3): Sejam a e m inteiros positivos relativamente primos . Então o menor inteiro positivo x tal que $a^x \equiv 1$ (*mod m*) é chamado a ordem de *a mod m*.
Notação: $ord_m a$.

Exemplo (4.2) Encontrar a ordem de 2 módulo 7, calculamos o menor resíduo positivo módulo 7 das potências de 2. Achamos que

$$2^1 \equiv 2 \pmod 7,\ 2^2 \equiv 4 \pmod 7,\ 2^3 \equiv 1 \pmod 7.$$

Portanto, $ord_7 2 = 3$.

Definição (4.4) Se r e n são inteiros relativamente primos com $n > 0$ e se $ord_n r = \phi(n)$, então r é chamado uma n raiz primitiva módulo n.

Exemplo (4.3) Vimos que $ord_7 3 = 6 = \phi(7)$, consequentemente, 3 é uma raiz primitiva módulo 7. Também, como $ord_7 5 = 6$, como pode ser verificado facilmente, 5 também é uma raiz primitiva módulo 7.

Definição (4.5) Seja m inteiro positivo com raiz primitiva r módulo m. Se a é inteiro positivo com (a, m) = 1, então o único inteiro x com $1 \leq x \leq \phi(m)$ e $r^x \equiv a \pmod m$ é chamado o expoente de a na base r *mod m*. Isso é, $a \equiv r^{ind_r a} \pmod m$.

Se x é o expoente de a na base r *módulo m*, então escrevemos $x = ind_r a$, onde não indicamos o módulo m na notação, pois é assumido ser fixo. Da definição, sabemos que se a e b são inteiros relativamente primos a m e $a \equiv b \pmod m$, então $ind_r a = ind_r b$.

Segue as propriedades do expoente de a na base r mod m:
Exemplo(4.4) Para $m = 7$. Vimos que 3 é uma raiz primitiva módulo 7 e que $3^1 \equiv 3$ (*mod* 7), $3^2 \equiv 2$ (*mod* 7), $3^3 \equiv 6$ (*mod* 7), $3^4 \equiv 4$ (*mod* 7), $3^5 \equiv 5$ (*mod* 7) e $3^6 \equiv 1$ (*mod* 7).

Consequentemente, módulo 7 temos

$$ind_3 1 = 6,\ ind_3 2 = 2,\ ind_3 3 = 1,\ ind_3 4 = 4,\ ind_3 5 = 5,\ ind_3 6 = 3.$$

Com uma raiz primitiva módulo 7 diferente, obtemos um conjunto diferente de expoentes.

Teorema (4.5) Seja m um inteiro positivo com raiz primitiva r e sejam a, b inteiros relativamente primos a m. Então

(i) $ind_r 1 \equiv 0\ (mod\ \phi(m))$.

(ii) $ind_r(ab) \equiv ind_r a + ind_r b\ (mod\ \phi(m))$.

(iii) $ind_r a^k \equiv k.\ ind_r a (mod\ \phi(m))$. *Se k é inteiro positivo.*

Prova.[ROSEN, 93] (i) Do teorema de Euler, sabemos que $r^{\phi(m)} \equiv 1\ (mod\ m)$. Já que r é uma raiz primitiva módulo m, nenhuma potência menor de r é congruente a 1 módulo m. Consequentemente, $ind_r 1 = \phi(m) \equiv 0\ (mod\ \phi(m))$.

(ii) Para provar essa congruência, note que da definição de índices

$$r^{ind_r(ab)} \equiv ab (\mathrm{mod}\, m)$$

e

$$r^{ind_r a + ind_r b} \equiv r^{ind_r a}.r^{ind_r b} \equiv ab (\mathrm{mod}\, m).$$

Consequentemente,

$$r^{ind_r(ab)} \equiv r^{ind_r a + ind_r b} (\mathrm{mod}\, m).$$

Conhecendo o resultado: sejam a e n inteiros relativamente primos, com $n > 0$, então $a^i \equiv a^j$ *(mod n)*, onde i e j são inteiros positivos, se e somente se $i \equiv j\ (mod\ ord_n a)$. Concluímos que

$$ind_r(ab) \equiv ind_r a + ind_r b\ (mod\ \phi(m)).$$

(iv) Para provar a congruência, primeiro note que, por definição, temos

$$r^{ind_r a^k} \equiv a^k (\mathrm{mod}\, m)$$

e

$$r^{k.ind_r a} \equiv \left(r^{ind_r a}\right)^k \equiv a^k (\mathrm{mod}\, m).$$

Usando o mesmo resultado dado para demonstrar o item anterior, isto nos conduz imediatamente à congruência que queremos, isto é,

$$ind_r a^k \equiv k.ind_r a (\mathrm{mod}\, \phi(m)).\square$$

Lema(4.1): Seja p um primo ímpar, α e q inteiros positivos. Então o número de soluções incongruentes da congruência $x^q \equiv 1 \pmod{p^\alpha}$ é $(q, p^{\alpha-1}(p-1))$.

Prova.[ROSEN, 93] Seja r raiz primitiva de p^α. Tomando expoentes referentes a r, vemos que $x^q \equiv 1 \pmod{p^\alpha}$ se, e somente se $qy \equiv 0 \pmod{\phi(p^\alpha)}$ onde $y = ind_r x$. Usando o Teorema 1.5 , vemos que existe exatamente $(q, \phi(p^\alpha))$ soluções incongruentes de $qy \equiv 0 \pmod{\phi(p^\alpha)}$. Consequentemente, existe $(q, \phi(p^\alpha)) = (q, p^{\alpha-1}(p-1))$ soluções incongruentes de $x^q \equiv 1 \pmod{p^\alpha}$.□

Estamos prontos para prova do teorema (4.4).

Prova.[ROSEN,93] Seja $n-1 = 2^s t$, com s inteiro positivo e t inteiro positivo ímpar. Para n ser um pseudo primo forte(definição 4.2) na base b, ou,

$$b^t \equiv 1 \pmod{n}$$

ou

$$b^{2^j t} \equiv -1 \pmod{n}$$

para algum inteiro j com $0 \leq j < s-1$. Em qualquer caso, temos

$$b^{n-1} \equiv 1 \pmod{n}.$$

Seja a fatoração em potências de primos de n

$$n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$$

Pelo lema (4.1), sabemos que existem

$$(n-1,\ p_j^{e_j-1}(p_j - 1)) = (n-1, p_j-1)$$

soluções incongruentes da congruência

$$x^{n-1} \equiv 1 \pmod{p_j^{e_j}}, \quad j = 1,2,\ldots, r.$$

O teorema Chinês dos restos, nos diz que existe exatamente

$$\prod_{j=1}^{r} (n-1, p_j-1)$$

soluções incongruentes para a congruência

$$x^{n-1} \equiv 1 \pmod{n}.$$

Para provar o teorema, primeiro consideramos o caso em que a fatoração em potências de primos de n contém uma potência de primo $p_k^{e_k}$ com expoente $e_k \geq 2$. Como

$$\left(p_k - 1\right) / p_k^{e_k} = \left(1 / p_k^{e_k - 1}\right) - \left(1 / p_k^{e_k}\right) \leq 2/9$$

(O maior valor possível ocorre quando $p_j = 3$ e $e_j = 2$), vemos que

$$\prod_{j=1}^{r}\left(n-1, p_j - 1\right) \leq \prod_{j=1}^{r}\left(p_j - 1\right)$$

$$\leq \left(\prod_{\substack{j=1 \\ j \neq k}}^{r} p_j\right)\left(\frac{2}{9} p_k^{e_k}\right)$$

$$\leq \frac{2}{9} n.$$

Do fato que $\frac{2}{9} n \leq \frac{1}{4}(n-1)$ para $n \geq 9$, segue que

$$\prod_{j=1}^{r}\left(n-1, p_j - 1\right) \leq (n - 1/4).$$

Consequentemente, existem no máximo *(n-1)/4* inteiros b, $1 \leq b \leq n$, para o qual n seja um pseudoprimo forte na base b.

O outro caso a considerar é quando $n = p_1 p_2 p_3 ... p_r$, onde p_1, p_2, ..., p_r são primos distintos. Seja

$$p_i - 1 = 2^{s_i} t_i, \quad i = 1, 2, ..., r,$$

em que s_i é inteiro positivo e t_i um inteiro positivo ímpar. Reordenamos os primos p_1, p_2, ..., p_r (se necessário) de forma que $s_1 \leq s_2 \leq ... \leq s_r$. Notamos que

$$(n-1, p_i - 1) = 2^{min(s, s_i)}\left(t, t_i\right).$$

O número de soluções incongruentes de $x^t \equiv 1 \ (mod\ p_i)$ é $T = (t,\ t_i)$. Há $2^j t_i$ soluções incongruentes para $x^{2^j t} \equiv -1 \left(\mathrm{mod}\ p_i\right)$ quando $0 \leq j \leq s_i - 1$, e nenhuma solução caso contrário. Consequentemente, usando o teorema Chinês dos restos, existem $T_1 T_2 ... T_r$ soluções incongruentes para $x^t \equiv 1 \ (mod\ n)$, e $2^{jr}\ T_1 T_2 ... T_r$ soluções incongruentes para $x^{2^j t} \equiv -1 \left(\mathrm{mod}\ p_i\right)$ quando $0 \leq j \leq s_1 - 1$. Então, existem um total de

$$T_1 T_2 ... T_r \left(1 + \sum_{j=0}^{s_1 - 1} 2^{jr}\right) = T_1 T_2 ... T_r \left(1 + \frac{2^{rs_1} - 1}{2^r - 1}\right)$$

inteiros b com $1 \leq b \leq n-1$, para que n ser um pseudoprimo forte na base b.

Note que

$$\phi(n) = (p_1-1)(p_2-1)\ldots(p_r-1) = t_1 t_2 \ldots t_r \, 2^{s_1+s_2+\ldots+s_r}.$$

Mostraremos que

$$T_1 T_2 \ldots T_r \left(1+\frac{2^{rs_1}-1}{2^r-1}\right) \leq \phi(n)/4,$$

que prova o resultado desejado. Porque $T_1 T_2 \ldots T_r \leq t_1 t_2 \ldots t_r$, podemos alcançar nossa meta mostrando que

$$\left(1+\frac{2^{rs_1}-1}{2^r-1}\right) / 2^{s_1+s_2+\ldots+s_r} \leq \tfrac{1}{4}. \qquad (4.1)$$

Como $s_1 \leq s_2 \leq \ldots \leq s_r$, vemos que

$$\left(1+\frac{2^{rs_1}-1}{2^r-1}\right) / 2^{s_1+s_2+\ldots+s_r} \leq \left(1+\frac{2^{rs_1}-1}{2^r-1}\right) / 2^{rs_1}$$

$$= \frac{1}{2^{rs_1}} + \frac{2^{rs_1}-1}{2^{rs_1}\left(2^r-1\right)}$$

$$= \frac{1}{2^{rs_1}} + \frac{1}{2^r-1} - \frac{1}{2^{rs_1}\left(2^r-1\right)}$$

$$= \frac{1}{2^r-1} + \frac{2^r-2}{2^{rs_1}\left(2^r-1\right)}$$

$$\leq \frac{1}{2^{r-1}}.$$

Dessa desigualdade concluímos que (4.1) é válida quando $r \geq 3$.

Quando $r = 2$, temos $n = p_1 p_2$, com $p_1 - 1 = 2^{s_1} t_1$ e $p_2 - 1 = 2^{s_2} t_2$, com $s1 \leq s2$, então (4.1) é novamente válida, pois

$$\left(1+\frac{2^{2s_1}-1}{3}\right) / 2^{s_1+s_2} = \left(1+\frac{2^{2s_1}-1}{3}\right) / \left(2^{2s_1} \cdot 2^{s_2-s_1}\right)$$

$$= \left(\frac{1}{3} + \frac{1}{3 \cdot 2^{2s_1-1}}\right) / 2^{s_2-s_1}$$

$$\leq \frac{1}{4}.$$

Quando $s_1 = s_2$, temos $(n-1, p_1-1) = 2^s T_1$ e $(n-1, p_2-1) = 2^s T_2$. Assumimos que $p_1 > p_2$. Note que $T_1 \neq t_1$, se $T_1 = t_1$, então $(p_1-1) \backslash (n-1)$, assim

$$n = p_1 p_2 \equiv p_2 \equiv 1 \ (mod \ (p_1 - 1)),$$

Que implica que $p_2 > p_1$, uma contradição. Já que $T_1 \neq t_1$, sabemos que $T_1 \leq t_1 / 3$. Similarmente, se $p_1 < p_2$ então $T_2 \neq t_2$, assim $T_2 \leq t_2 / 3$. Consequentemente, $T_1 T_2 \leq t_1 t_2 / 3$, e como $\left(1 + \frac{2^{2s_1} - 1}{3}\right) / 2^{2s_1} \leq \frac{1}{2}$, temos

$$T_1 T_2 \left(1 + \frac{2^{2s_1} - 1}{3}\right) \leq t_1 t_2 2^{2s_1} / 6 = \phi(n) / 6,$$

provando o teorema para esse caso final, pois $\phi(n)/6 \leq (n-1)/6 < (n-1)/4$.□

Analisando as desigualdades na prova do Teorema (4.4), podemos ver que a probabilidade de n ser um pseudoprimo forte para as bases b, $1 \leq b \leq n-1$ escolhidas aleatoriamente, está perto de 1/4 para inteiros n com fatoração em primos da forma $n = p_1 p_2$ com $p_1 = 1 + 2q_1$ e $p_2 = 1 + 4q_2$, onde q_1 e q_2 são primos ímpares ou $n = q_1 q_2 q_3$ com $p_1 = 1 + 2q_1$, $p_2 = 1 + 2q_2$, e $p_3 = 1 + 2\,q_3$, onde q_1, q_2, e q_3 são primos ímpares distintos.

Do Teorema (4.4), vemos que se n é composto a probabilidade que n passe no teste de Miller para a base b é menor que 1/4. Se escolhemos k diferentes bases menores que n e executamos o teste de Miller para cada uma destas bases somos conduzidos ao seguinte resultado.

Teorema (4.6). (Teste de Primalidade Probabilístico de Miller - Rabin.) Seja n um inteiro positivo. Escolha k diferentes inteiros positivos menores que n e execute o teste de Miller em n para cada uma destas bases. Se n é composto a probabilidade que n passe todos os testes k é menor que $(1/4)^k$.

Exemplo (4.5) Se $k = 50$, então a probabilidade de erro é, no máximo, $1/2^{100}$. Isso significa que, se o teste é aplicado a $m = 2^{100}$ inteiros $n_1, n_2, \ldots, n_m$, então o número esperado de resposta errada seja uma. Isso mostra que usando o teste de Miller - Rabin não teremos uma prova definitiva que um determinado número n é primo, mas sim uma evidência extremamente forte.

O ponto importante relativo ao teste de primalidade probabilístico de Miller - Rabin e o Teorema 4.4 é que ambos resultados indicam que é possível testar se um inteiro n é primo usando apenas $O((\log_2 n)^k)$ operações, onde k é um inteiro positivo.

Na prática, entretanto, podemos deparar com um número ímpar grande n, do qual não estamos seguros se é primo ou composto. Suponha que escolhemos um número qualquer $b \in [1, n-1]$ e sendo

$$\varphi(n) = \{ b \in [1, n-1] : b^t \equiv 1 \ (mod\ n) \ ou \ b^{2^j t} \equiv -1 \ (mod\ n) \ para\ j < t \},$$

se $b \in \varphi(n)$, poderíamos escolher outro número $b' \in [1, n-1]$ e tentar novamente. Do teorema de Miller - Rabin, temos o seguinte: a probabilidade que um número composto ímpar n tenha $b_1, \ldots, b_t \in \varphi(n)$ para $b_1, \ldots, b_t$ escolhido aleatoriamente e independentemente dos inteiros em $[1, n-1]$ é no máximo 4^{-t}, onde t é o número de tentativas.

O teste de primalidade que é nosso objeto de pesquisa se fundamenta também na irredutibilidade dos polinômios de Chebyshev. Por esta razão, o próximo capítulo será dedicado a definição e propriedades destes polinômios.

5- Propriedades Algébricas dos Polinômios de Chebyschev

Estabeleceremos primeiro definições e propriedades dos polinômios de Chebyshev do primeiro e segundo tipo, necessárias para nossos principais resultados. Em particular, serão desenvolvidos critérios para determinar a irredutibilidade e fatoração dos polinômios de Chebyshev sobre os inteiros Z. Também apresentaremos, testes para decidir quando um polinômio de Chebyshev é dividido por outro, terminando com um procedimento para computar as raízes modulares.

5.1- Definições e propriedades

Definição (5.1): Os polinômios de Chebyshev de primeiro tipo $T_n(x)$ são definidos por

$$T_n(x) = \cos n\,(\arccos x) = \cos n\theta$$

$$x = \cos\theta$$

em que $0 \leq \theta \leq \pi$. As raízes de $T_n(x)$ são reais, distintas, no intervalo $[\,-1,\ 1\,]$ e determinadas pela seguinte fórmula

$$\xi_k = \cos\frac{(2k-1)}{n}\frac{\pi}{2},\ k = 1, \ldots, n. \qquad (5.1)$$

As raízes ξ_k são simétricas com relação a linha $x = 0$. Em outras palavras, se x for uma raiz de $T_n(x)$, então $-x$ também será.

Usando identidades trigonométricas, podemos calcular os polinômios de Chebyshev de primeiro tipo diretamente:

$$T_0(x) = \cos 0 = 1$$

$$T_1(x) = \cos\theta = x$$

$$T_2(x) = \cos 2\theta = \cos\theta\cos\theta - \operatorname{sen}\theta\operatorname{sen}\theta = \cos^2\theta - \operatorname{sen}^2\theta =$$

$$= \cos^2\theta - (1 - \cos^2\theta) = 2\cos^2\theta - 1 = 2x^2 - 1.$$

Para calcular $T_n(x)$, para um valor elevado de n é mais simples fazer uso da fórmula de recorrência para $T_n(x)$:

$$T_{n+1}(x) = 2x\,T_n(x) - T_{n-1}(x), \tag{5.2}$$

para estabelecermos (5.2), temos

$$T_{n+1}(x) = \cos(n+1)\theta = \cos n\theta\cos\theta - \operatorname{sen} n\theta\operatorname{sen}\theta$$

$$T_{n-1}(x) = \cos(n-1)\theta = \cos n\theta\cos\theta + \operatorname{sen} n\theta\operatorname{sen}\theta.$$

Adicionando-se membro a membro as expressões acima, temos

$$T_{n+1}(x) + T_{n-1}(x) = 2\cos n\theta\cos\theta = 2x\,T_n(x)$$

$$T_{n+1}(x) = 2x\,T_n(x) - T_{n-1}(x)$$

Logo

$$T_n(x) = 2xT_{n-1}(x) - T_{n-2}(x), \text{ com } n = 2, 3, \ldots \tag{5.3}$$

Que verifica (5.2) e para $n = 3$, temos

$$T_3(x) = 2xT_2(x) - T_1(x) = 2x(2x^2-1) - x = 4x^3 - 3x$$

Podemos desta maneira, gerar $T_n(x)$ para qualquer n. Na tabela abaixo, os primeiros oito polinômios são apresentados na coluna A e a coluna B mostra que o coeficiente de x^n em $T_n(x)$ é 2^{n-1}, definindo uma propriedade :

A	B
$T_0(x) = 1$	$1 = T_0$
$T_1(x) = x$	$x = T_1$
$T_2(x) = 2x^2 - 1$	$x^2 = 2^{-1}(T_0 + T_2)$
$T_3(x) = 4x^3 - 3x$	$x^3 = 2^{-2}(3T_1 + T_3)$
$T_4(x) = 8x^4 - 8x^2 + 1$	$x^4 = 2^{-3}(3T_0 + 4T_2 + T_4)$
$T_5(x) = 16x^5 - 20x^3 + 5x$	$x^5 = 2^{-4}(10T_1 + 5T_3 + T_5)$
$T_6(x) = 32x^6 - 48x^4 + 18x^2 - 1$	$x^6 = 2^{-5}(10T_0 + 15T_2 + 6T_4 + T_6)$
$T_7(x) = 64x^7 - 112x^5 + 56x^3 - 7x$	$x^7 = 2^{-6}(35T_1 + 21T_3 + 7T_5 + T_7)$

As propriedades seguintes são úteis na fatoração dos polinômios de Chebyshev de primeiro tipo.

$$T_{mn}(x) = T_m(T_n(x)), \text{ com } m,n \geq 0 \tag{5.4}$$

Prova. Considerando $m > n \geq 0$, temos que

$$T_m(T_n(x)) = \cos m\,(\arccos\,(T_n(x)) = \cos m\,(\,\arccos \cos n \arccos x\,))$$
$$= \cos m\,(\,\arccos\,(\cos n\theta)\,) = \cos m\,(n\theta) = \cos mn\theta = T_{mn}(x).\square$$

$$T_m(x)T_n(x) = \tfrac{1}{2}(\,T_{m+n}(x) + T_{|m-n|}(x)\,)\,,\ com\ m,n \geq 0 \qquad (5.5)$$

Prova. Considerando $m > n \geq 0$, temos que

$$T_{m+n}(x) = \cos\,(m+n)\theta = \cos m\theta \cos n\theta - \operatorname{sen} m\theta \operatorname{sen} n\theta \ \ e$$
$$T_{m-n}(x) = \cos\,(m-n)\ \theta = \cos m\theta \cos n\theta + \operatorname{sen} m\theta \operatorname{sen} n\theta.$$

Adicionando-se membro a membro as expressões acima, temos

$$T_{m+n}(x) + T_{m-n}(x) = 2\cos m\theta \cos n\theta = 2\,T_m(x)\,T_n(x) = 2\,T_{mn}(x).\square$$

Podemos também definir $T_{-n}(x)$ como segue:

$$T_{-n}(x) = \cos\,(-n\theta) = \cos n\theta = T_n(x) \qquad (5.6)$$

Definição (5.2): Os polinômios de Chebyshev do segundo tipo são definidos fixando

$$U_0(x) = 1 \ \ e\ U_1(x) = 2x$$

e a relação de recorrência:

$$U_n(x) = 2x\,U_{n-1}\,(x) - U_{n-2}\,(x), \qquad n = 2,3,\ldots \qquad (5.7)$$

Eles também podem ser definidos como segue

$$U_n(x) = \frac{1}{n+1}T'_{n+1}(x) = \frac{\operatorname{sen}((n+1)\arccos x)}{\operatorname{sen}(\arccos x)}. \qquad (5.8)$$

$U_n(x)$ são polinômios inteiros de grau n. Suas raízes são todas reais, distintas, simétricas com relação a linha $x = 0$ e são dadas pela expressão:

$$\eta_k = \cos\frac{k\pi}{n+1} \ \text{com}\ k = 1, \ldots, n \qquad (5.9)$$

Propriedades úteis da decomposição dos polinômios $U_n(x)$ incluem as seguintes:

$$U_{mn-1}(x) = U_{m-1}(\,T_n(x)\,)U_{n-1}(x),\ \ m,n > 0 \qquad (5.10)$$

Prova. Temos que, $U_{mn-1}(x) = \dfrac{\operatorname{sen} mn\theta}{\operatorname{sen}\theta}$ e

$$U_{m-1}(T_n(x))U_{n-1}(x) = \frac{\operatorname{sen} m\left(\arccos\left(T_n(x)\right)\right)}{\operatorname{sen}\left(\arccos\left(T_n(x)\right)\right)}U_{n-1}(x) = \frac{\operatorname{sen} m(\arccos\cos n\theta)}{\operatorname{sen} n\theta}U_{n-1}(x) = \frac{\operatorname{sen} mn\theta}{\operatorname{sen} n\theta} =$$

$$= \frac{\operatorname{sen} mn\theta}{\operatorname{sen} n\theta}\cdot\frac{\operatorname{sen}\theta}{\operatorname{sen}\theta}U_{n-1}(x) = \frac{\operatorname{sen} mn\theta}{\operatorname{sen}\theta}\cdot\frac{\operatorname{sen}\theta}{\operatorname{sen} n\theta}U_{n-1}(x) = U_{mn-1}(x)\frac{1}{U_{n-1}(x)}U_{n-1}(x) = U_{mn-1}(x).$$

$$T_n(x)U_{m-1}(x) = \tfrac{1}{2}\left(U_{m+n-1}(x) + U_{m-n-1}(x)\right),\ m > n > 0. \qquad (5.11)$$

Prova. Temos que, $2T_n(x)U_{m-1}(x) = 2\cos n\theta\dfrac{\operatorname{sen} m\theta}{\operatorname{sen}\theta}$ e

$$U_{m+n-1}(x) = \frac{\operatorname{sen}(m+n)\theta}{\operatorname{sen}\theta} = \frac{\operatorname{sen} m\theta\cdot\cos n\theta + \operatorname{sen} n\theta\cdot\cos m\theta}{\operatorname{sen}\theta};$$

$$U_{m-n-1}(x) = \frac{\operatorname{sen}(m-n)\theta}{\operatorname{sen}\theta} = \frac{\operatorname{sen} m\theta\cdot\cos n\theta - \operatorname{sen} n\theta.\cos m\theta}{\operatorname{sen}\theta}.$$

Adicionando-se membro a membro as duas expressões acima, temos

$$U_{m+n-1}(x) + U_{m-n-1}(x) = 2\cos n\theta\frac{\operatorname{sen} m\theta}{\operatorname{sen}\theta} = 2T_n(x)U_{m-1}(x).\square$$

Para estender a definição dos polinômios de Chebyshev do segundo tipo para n negativo, note que para $n > 1$

$$U_{-n}(x) = \frac{1}{-n+1}T'_{-n+1}(x) = -\frac{1}{n-1}T'_{-(n-1)}(x) = -\frac{1}{n-1}T'_{(n-1)}(x) = -U_{n-2}(x). \qquad (5.12)$$

A próxima seção apresenta condições para a determinação da divisibilidade de um polinômio de Chebyshev por outro através de propriedades. Em particular, mostra também, que o resto da divisão de um polinômio de Chebyshev é, senão zero, outro polinômio de Chebyshev.

5.2 – Divisão entre polinômios de Chebyshev

Começaremos com os polinômios de Chebyshev de primeiro tipo $T_n(x)$:

Propriedade (i) Seja $n > 1$ um inteiro. Se h é qualquer divisor ímpar de n, então $T_{n/h}(x)$ é um divisor de $T_n(x)$.

Prova. Seja $n = kh$, h ímpar. Aplicando a decomposição da propriedade (5.4), temos que

$$T_n(x) = T_{kh}(x) = T_h(T_k(x)) = a_h[T_k(x)]^h + \ldots + a_1[T_k(x)]^1 + 0.\square$$

Sejam $T_m(x)$ e $T_n(x)$ dois polinômios de Chebyshev do primeiro tipo. Executando a divisão de Euclides, obtemos os polinômios quociente $q(x)$ e o resto $r(x)$ satisfazendo

$$T_m(x) = q(x)T_n(x) + r(x), \quad \text{com} \quad grau(r) < grau(T_n). \tag{5.13}$$

$q(x)$ e $r(x)$ podem ser determinados usando os seguintes resultados,

Lema 1. Sejam $m \geq n$ inteiros positivos. Se m não é um múltiplo ímpar de n, então existe um único inteiro positivo l tal que $|m - 2ln| < n$.

Prova. Já que m não é um múltiplo ímpar de n, $\exists\, l$ tal que

$$(2l-1)n < m < (2l+1)n.$$

Manipulando-se as desigualdades, chegamos à

$$-n < m - 2ln < n. \square$$

Propriedade (ii) Sejam $m \geq n$ dois inteiros positivos. Os polinômios $q(x)$ e $r(x)$ pela divisão de Euclides (5.13) são dados por

$$q(x) = 2\sum_{k=1}^{l}(-1)^k T_{m-(2k-1)n}(x)$$

$$r(x) = (-1)^l T_{|m-2ln|}(x),$$

se existe um inteiro $l \geq 1$ que satisfaça $|m - 2ln| < n$, caso contrário,

$$q(x) = 2\sum_{k=1}^{l-1}(-1)^k T_{m-(2k-1)n}(x) + (-1)^{l-1}$$

$$r(x) = 0,$$

em que l satisfaz $m = (2l-1)n$.

Prova. [RAYES, 98] Substituindo m por m-n na equação (5.5) e usando a definição estendida (5.6), temos

$$T_m(x) = 2T_n(x)T_{m-n}(x) - T_{m-2n}(x), \text{ com } m, n \text{ inteiros.} \qquad (5.14)$$

Seja l o único inteiro positivo que satisfaz $(2l-1)\ n \leq m \leq (2l+1)n$. Aplicando a fórmula de decomposição (5.5) $l - 1$ vezes, deduzimos

$$T_m(x) = 2T_n(x)\{ T_{m-n}(x) - T_{m-3n}(x) + \ldots + (-1)^{l-1}T_{m-(2l-3)n}(x) \} + (-1)^{l-1}T_{m-(2l-2)n}(x).$$

Se $(2l-1)n < m$, então $grau(T_n(x)) < grau(T_{m-(2l-2)n}(x))$ e podemos aplicar propriedade(5.14) mais uma vez, provando o primeiro caso. Por outro lado, se $m = (2l-1)n$, então $m-(2l-2)n = -n$. Segue que $r(x) = 0$ e o segundo caso é demonstrado. □

Da propriedade acima, vemos que o resto da divisão de dois polinômios de Chebyshev do primeiro tipo é zero ou outro polinômio de Chebyshev do primeiro tipo (a menos de sinal). Também podemos deduzir da propriedade (ii) que, se $T_n(x)$ é um divisor de $T_m(x)$ então n é um divisor ímpar de m. Esta afirmação pode ser vista como a recíproca da propriedade (i). O seguinte teorema resume os resultados.

Teorema (5.1) Para os inteiros $0 < n \leq m$, $T_n(x)$ é um divisor de $T_m(x)$ se e somente se $m = (2l - 1)\ n$ para algum inteiro $l > 1$. Caso contrário, o resto da divisão de Euclides de $T_m(x)$ por $T_n(x)$ é determinado através de $r(x) = (-1)^l\ T_{|m-2nl|}(x)$, em que l é o único inteiro que satisfaz $|m-2nl| < n$.

E agora os polinômios de Chebyshev de segundo tipo $U_n(x)$:

Propriedade (iii) $U_n(x)$ é um divisor de $U_m(x)$ se existir um inteiro $l > 0$ tal que $m = ln + l - 1$.

Prova.[RAYES, 98] $U_m(x) = U_{l(n+1)-1}(x) = U_{l-1}(T_n(x))U_n(x)$.□

Para determinarmos a divisão de Euclides de $U_m(x)$ por $U_n(x)$, usamos a definição estendida para indices negativo de polinômios de Chebyshev e aplicando equação (5.12) com $m + n - 1$ substituído por m e $m-1$ substituído por n.

$$U_m(x) = 2T_{m-n}(x)U_n(x)-U_{2n-m}(x), \quad \text{com } m, n \text{ inteiros.} \tag{5.15}$$

Porque $U_{-1}(x) = 0$, a equação acima também vale para $2n-m = -1$. Para $m = n$, podemos escrever $U_m(x) = (2T_{m-n}(x) - 1)U_n(x)$. Também note que $2n-m \leq n$ e se $2n - m \geq -1$ temos o resto e quociente determinados. Por outro lado, se $2n-m \leq -2$, podemos aplicar a definição estendida para $U_{2n-m}(x)$. Resumindo, temos

$$U_m(x) = \begin{cases} 2T_{m-n}(x)U_n(x) - U_{2n-m}(x), & se \quad n \leq m \leq 2n+1 \\ 2T_{m-n}(x)U_n(x) + U_{m-2n-2(x)}, & se \quad 2n+2 \leq m < 3n+2 \end{cases} \tag{5.16}$$

Se $m \geq 3n+2$, aplicamos a fórmula dada pela equação(5.15) novamente. Em geral, temos

Propriedade (iv) Sejam $m \geq n$ inteiros positivos. Se existir um inteiro $l \geq 0$ que satisfaz $(2l+1)n+2l \leq m \leq (2l+2)n + 2l + 1$, então,

$$U_m(x) = 2U_n(x)\sum_{k=0}^{l} T_m - (2k+1)n - 2k(x) - U_{2(l+1)n-m-2l}(x),$$

caso contrário

$$U_m(x) = 2U_n(x)\sum T_{m-(2k+1)n-2k}(x) + U_{2(l+1)n-m-2l}(x),$$

em que m satisfaz $(2l+2)n + 2l + 2 \leq m < (2l+3)n + 2l + 2$, quando $m = (2l+1)n + 2l$, a equação acima pode ser reescrita como

$$U_m(x) = U_n(x)\left(2\sum_{k=0}^{l} T_{m-(2k+1)n-2k}(x) - 1\right),$$

e temos, da propriedade (iii), resto zero. Se $m = (2l+2)n + 2l + 1$, temos resto zero novamente (porque $U_{-1}(x) = 0$). Em todos os outros casos, o primeiro termo das equações dadas na propriedade (iv) determina o quociente da divisão de Euclides de U_m por U_n, enquanto o segundo termo dá o resto(não nulo). Usando a definição estendida (5.6), demonstramos o seguinte

Teorema(5.2) Sejam $m \leq n$ inteiros positivos. $U_m(x)$ é um múltiplo de $U_n(x)$ se e somente se $m = (l+1)n + 1$ para algum inteiro $l \geq 0$. Caso contrário, o resto da divisão de Euclides

de $U_m(x)$ por $U_n(x)$ é determinado através do $r(x) = -U_{2(l+1)n-m-2l}(x)$, onde $l \geq 0$ satisfazem $(l+1)n + l < m < (l+3)n + l + 2$.

Exemplo(5.1): Considere m = 33 e n = 4. Como $30 = 6.4 + 6 \leq 33 < 7.4 + 6 = 34$, usamos a segunda fórmula de propriedade (iv) e determinamos que

$$U_{33}(x) = 2\,U_4(x)(T_{29}(x) + T_{19}(x) + T_9(x) + U_3(x)$$

5.3- A Fatoração dos polinômios de Chebyshev sobre Z

Usando um resultado de D.H. Lehmer, H. J. Hsiao determinou a fatoração dos polinômios de Chebyshev de primeiro tipo $T_n(x)$ sobre Z, determinando quais raízes deveriam ser agrupadas para resultar em fatores irredutíveis com coeficientes inteiros. Aqui, um resultado similar para os polinômios de Chebyshev de segundo tipo $U_n(x)$ é derivado. Com uma pequena modificação em termos de notação, o resultado de Hsiao segue

Teorema (5.3): (Hsiao) Seja $n > 1$ um inteiro. Então

$$T_n(x) = 2^{n-1} \prod_h D_h(x),$$

Onde $h \leq n$ percorre todos os divisores positivos de n e

$$D_h(x) = \prod_{\substack{k=1 \\ (2k-1,n)=h}}^{n} \left(x - \xi_k\right) \tag{5.17}$$

são polinômios irredutíveis sobre os racionais.

Prova. De D. H. Lehmer[LEHMER, 33], sabemos que: se $L > 2$ e $(k, L) = 1$, então $2\cos\frac{2k\pi}{L}$ é algébrico e de grau $\phi(L)/2$. Para $k=1$ e $L = 4n$, obtemos $2\cos\frac{\pi}{2n}$ é algébrico de grau $\phi(4n)/2$. Da prova do resultado de Lehmer, também vemos que todos ξ_k com $(2n, 2k - 1) = 1$ são raízes do mesmo polinômio irredutível. Multiplicando esse polinômio por 2^{l_1}, onde $l_1 = \phi(4n)/2$, obtemos $D_1(x)$ é um polinômio irredutível sobre Z. Seja $h > 1$ um

divisor ímpar de n. Então, para cada inteiro ímpar $2k-1$, com $1 \leq k \leq n$ satisfazendo $(2k-1, 2n) = h$, corresponde inteiro ímpar $2i - 1 = (2k-1) / h$ com $1 \leq i \leq n / h$ satisfazendo $(2i-1, 2n/h) = 1$. A recíproca também é verdadeira. Logo, com o mesmo argumento do parágrafo anterior, todas as ξ_k com $1 \leq 2k - 1 \leq 2n - 1$ satisfazendo $(2k-1, n) = h$ são raízes do mesmo polinômio irredutível de grau $N = \phi(4n / h) / 2$. Para obtermos um polinômio inteiro, basta multiplicar pela constante 2^{n-1}. Como cada raiz ξ_k de $T_n(x)$ é raiz de um único $D_h(x)$, com $h = (2k-1, n)$, o resultado fica provado. □

Aplicando o mesmo método usado por Hsiao, provamos um resultado similar para

os polinômios de Chebyshev de segundo tipo $U_n(x)$. Considere um inteiro $n \geq 2$. Seja $h \leq n$ um divisor positivo de $2n + 2$ e l_h o número de elementos do conjunto

$$S_h = \{ k : (k, 2n + 2) = h, 1 \leq k \leq n \}.$$

É fácil ver que $l_h = \# (S_h) = \phi ((2n + 2)/h)/2$.

Seja

$$E_h(x) = 2^{l_h} \prod_{\substack{k=1 \\ (k,2n+2)=h}}^{n} \left(x - \eta_k\right), \tag{5.18}$$

em que η_k são os zeros de $U_n(x)$ definidos na equação (5.9).

Teorema (5.4): Para qualquer inteiro $n \geq 2$, $U_n(x)$ tem a fatoração

$$U_n(x) = \prod_h E_h(x), \text{ em que } h \leq n$$

percorre todos os divisores positivos $2n + 2$. Os E_h são irredutíveis sobre os inteiros.

Prova. [RAYES, 99] De D. H. Lehmer, sabemos que: Se $L > 2$ e $(k, L) = 1$, então 2 cos $\frac{2k\pi}{L}$ é algébrico de grau $\phi(L)/2$. Seja $k=1$ e $L = 2n + 2$, obtemos que 2 cos $\frac{\pi}{n+1}$ é algébrico de grau $\phi(2n+2)/2$, ou que η_1 é algébrico de grau $\phi(2n+2)/2$. Da prova do resultado de Lehmer, também vemos que todos η_k com $(k, 2n+2) = 1$ são raízes do mesmo polinômio irredutível. Multiplicando esse polinômio por 2^{l_1}, em que $l_1 = \phi(2n+2)/2$,

obtemos que $E_1(x)$ é um polinômio irredutível sobre Z. Seja $h > 1$ um divisor de $2n + 2$. Considere todos $1 \leq k \leq n$ com $(k, 2n + 2) = h$. Para cada i, $k/h \leq i \leq \lfloor n / h \rfloor$ tal que$(i, (2n+2) / h) = 1$ e vice e versa. Assim pelo mesmo argumento do parágrafo anterior, todos os η_k, com $(k, 2n+2) = h$ são raízes do mesmo polinômio irredutível(racional) $E_h'(x)$ de grau $l_h = \phi((2n+2)/h)/2$. Multiplicando $E_h'(x)$ por 2^{l_h}, obtemos o polinômio inteiro $E_h(x)$. Uma raiz η_k de $U_n(x)$ é uma raiz de um único $E_h(x)$ onde $h = (k, 2n+2)$. □

Usando os teoremas (5.3) e (5.4), podemos agrupar as raízes dos polinômios de Chebyshev para obter seus fatores irredutíveis.

Exemplo (5.2). Suponha $n = 6$. $D_1(x)$ é formado da seguinte maneira: tomando as raízes ξ_1, ξ_3, ξ_4 e ξ_6, enquanto $D_3(x)$ é obtido juntando ξ_2 e ξ_5. Similarmente, $\xi_{51}(x)$ e $\xi_{52}(x)$ são obtidos tomando-se as raízes η_1, η_3, η_5 e η_2, η_4, η_6, respectivamente, obtemos os fatores inteiros:

$$T_6(x) = (2x^2 - 1) (16 x^4 - 16x^2 + 1)$$

$$U_6(x) = (8x^3 - 4x^2-4x + 1)(8x^3 + 4x^2-4x-1).$$

Corolário (5.1). Seja n um inteiro positivo.

1) $D_1(x)$ é o fator irredutível de $T_n(x)$ de maior grau é igual a $\phi(n)$.
2) $E_1(x)$ é o fator irredutível de $U_n(x)$ de maior grau é igual a $\phi(2n+2)/2$.

Corolário (5.2) Seja n um inteiro positivo.

1) O número de fatores irredutíveis de $T_n(x)$ é igual ao número de divisores ímpares de n.
2) O número de fatores irredutíveis de $U_n(x)$ é igual ao número de divisores $h \leq n$ de $2n+2$.

Então, um terceiro corolário pode ser deduzido.

Corolário (5.3) Seja n um inteiro positivo.

(1) $T_n(x)$ é irredutível se, e somente se, n for uma potência de 2.
(2) $U_n(x)$ é redutível para todos os $n > 1$.

Prova.[RAYES, 99] O único divisor ímpar de uma potência de 2 é 1. Se n não é uma potência de 2, então n tem no mínimo, dois divisores ímpares. Isso prova (1). Para provar (2) observe que para qualquer $n > 1$, 1 e 2 são divisores de $2n + 2$, então $U_n(x)$ tem pelo menos 2 fatores irredutíveis.□

No próximo capítulo, usaremos estes resultados para propor um teste de primalidade.

5.4- Fatoração modular

Consideraremos a fatoração dos polinômios de Chebyshev sobre corpos finitos Z_p. Especificamente, mostraremos a existência de primos p para qual $T_n(x)$ (ou $U_n(x)$) se decompõem em fatores lineares em Z_p. Sejam ξ_k as raízes de $T_n(x)$ definidas na equação (5.1), para $k = 1,...,n$, para algum n fixo. Note que

$$\xi_k = \cos\frac{2\pi}{4n}(2k-1),$$

ou

$$\xi_k = \frac{\left(e^{i\frac{2\pi}{4n}}\right)^{2k-1} + \left(e^{-i\frac{2\pi}{4n}}\right)^{2k-1}}{2} = \frac{w^{2k-1} + w^{-2k+1}}{2},$$

em que $w = e^{i\frac{2\pi}{4n}}$ é a $(4n)^{th}$ raiz complexa da unidade. Considere o corpo $Q(w)$, os racionais associados por w. Conhecemos por definição que

$$Q(w) = \{ (a_0/b_0) + (a_1/b_1)w + ... + (a_{s-1} / b_{s-1}) w^{s-1} : a_j, b_j \in Z \},$$

em que $s = [Q(w):Q]$ é o grau da extensão do corpo $Q(w)$ sobre Q. Sabe-se que $s = \phi(4n)$. Como observação, verificamos que o resultado de Lehmer mostra que $[Q(w):Q(w+1/w)] = 2$. Seja p um primo ímpar. Definimos

$$Q_{\bar{p}}(w) = \{ (a_0/b_0)+(a_1/b_1)w+ ...+ (a_{s-1}/ b_{s-1})w^{s-1} : a_j, b_j \in Z, p \nmid b_j \}.$$

É fácil ver que, $Q_{\bar{p}}(w)$ *é um anel.* Além disso, todas as potências de w, inclusive negativas, pertencem a $Q_{\bar{p}}(w)$. Seja $GF(q)$ um corpo finito de característica p com q elementos (q é uma potência de p). Assumimos que $GF(q)$ tem uma $(4n)^{th}$ raiz primitiva da unidade θ. Definindo o homomorfismo natural de anéis

$$\Psi: Z \rightarrow Z_p$$

por $\Psi(a) = a \bmod p$, podemos extender ao anel polinomial $Q_{\bar{p}}(w)[x]$ sobre $GF(q)[x]$ do seguinte modo.

$$\Psi(a/b) = \Psi(a)/\ \Psi(b)$$

$$\Psi(w) = \theta$$

$$\Psi(x) = x.$$

Com isto, temos que

$$\Psi(T_n(x)) = \Psi(\ 2^{n-1}(x - \xi_1)\ldots(x-\xi_n))$$

$$= \Psi\left(2^{n-1}\left(x-\frac{w+w^{-1}}{2}\right)\left(x-\frac{w^3+w^{-3}}{2}\right)\ldots\left(x-\frac{w^{2n-1}+w^{-2n+1}}{2}\right)\right)$$

$$= \Psi(2)^{n-1}\left(x-\frac{\theta-\theta^{-1}}{\psi(2)}\right)\left(x-\frac{\theta^3+\theta^{-3}}{\psi(2)}\right)\ldots\left(x-\frac{\theta^{2n-1}+\theta^{-2n+1}}{\psi(2)}\right).$$

Como as quantidades $\dfrac{\theta^{2k-1}+\theta^{-2k+1}}{\psi(2)}$ são bem definidas em $GF(q)$, vemos que $\Psi(T_n(x))$ tem todas suas raízes em $GF(q)$. Consequentemente, podemos encontrar n fatores lineares de $T_n(x)$ módulo um primo ímpar p, se qualquer uma das duas circunstâncias seguintes acontece. (i) O próprio corpo Z_p tem uma $(4n)^{th}$ raiz primitiva da unidade. (ii) $GF(q)$, um corpo com p característico, tem uma $(4n)^{th}$ raiz primitiva da unidade e todas as quantidades $\theta^{2j-1} - \theta^{-2j+1}$, $j = 1,\ldots, n$, pertençam ao corpo de base Z_p.

Lema (5.2) Sejam n e K inteiros positivos. Se $p = 4nK+1$ é primo, então Z_p tem uma $(4n)^{th}$ raiz primitiva da unidade.

Prova.[RAYES, 98] Um resultado bem conhecido estabelece que Z_p tem uma $(M)^{th}$ raiz primitiva da unidade se, e somente se M divide $p-1$ (ver, exemplo [Lidl,94], 81).□

Lema (5.3) Sejam n e K inteiros positivos. Se $p = 4nK-1$ é primo, então $GF(p^2)$ tem uma $(4n)^{th}$ raiz primitiva da unidade θ e todas as quantidades $\theta^{2j-1} - \theta^{-2j+1}$, $j = 1,\ldots, n$, pertençam ao corpo de base Z_p.

Prova. [RAYES, 98] Do fato que $4n$ divide p^2-1 segue a existência de θ, uma $(4n)^{th}$ raiz primitiva da unidade em $GF(p^2)$. Seja $f(x) = x^2 + ax + b$ um polinômio irredutível em $Z_p[x]$ e seja α uma raiz de $f(x)$. Considerando a aritmética de $GF(p^2) = Z_p[x]$, denotamos $\theta = c + d\,\alpha$, para algum $c, d \in Z_p$ e calcule $\theta^{-1} = \dfrac{c - da - d\alpha}{c^2 - cda + d^2b}$. Segue que

$$\theta + \theta^{-1} = c + \frac{c - ad}{c^2 - cda + d^2b} + \alpha\left(d - \frac{d}{c^2 - cda + d^2b}\right).$$

Para mostrar que $\theta + \theta^{-1} \in Z_p$ basta mostrar que $c^2 - cda + d^2b = 1$. Pela técnica do lema 5.4 abaixo observamos que $\theta^{p+1} = c^2 - cda + d^2b$. Como $p+1 = 4nk$ e θ é uma $(4n)^{th}$ raiz primitiva da unidade, segue que $c^2 - cda + d^2b = 1$. Da identidade

$$\theta^j + \theta^{-j} = (\theta + \theta^1)(\theta^{j-1} + \theta^{-(j-1)}) - (\theta^{j-2} + \theta^{-(j-2)}),$$

segue que todas as outras quantidades $\theta^{2j-1} + \theta^{(2j-1)}$ pertencem a Z_p. □

Lema (5.4). Seja p primo. Seja $\alpha \in GF(p^2)$ uma raiz do polinômio irredutível $f(x) = x^2 + ax + b$ sobre Z_p. Para qualquer $c, d \in Z_p$, temos

$$(c + d\alpha)^{p+1} = c^2 - cda + d^2b \in Z_p.$$

Prova.[RAYES, 98] Como a aritmética é feita módulo p, temos

$$(c + d\alpha)^{p+1} = \sum_{j=0}^{p+1} \binom{p+1}{j} c^j (d\alpha)^{p+1-j}$$

$$= c^{p+1} + (p+1)c^p d\alpha + (p+1)c(d\alpha)^p + (d\alpha)^{p+1}$$

$$= c^2 + cd\alpha + cd\alpha^p + d^2\alpha^{p+1}.$$

A última igualdade é uma conseqüência do pequeno teorema de Fermat. Observando que α^p é a outra raiz distinta de $f(x)$, vemos que $-a = \alpha + \alpha^p$, $b = \alpha^{p+1}$ e o resultado segue.□

Teorema (5.5) Seja $n \geq 2$ um inteiro. Para todos os infinitos inteiros positivos K para qual $p = 4nK \pm 1$ é um número primo, $T_n(x)$ tem n raízes em Z_p.

Precisaremos do seguinte teorema, na demonstração do teorema 5.5.

Teorema (5.6) (Dirichlet) Se l e m são inteiros com $(l,m) = 1$, então existem infinitos números primos satisfazendo $p \equiv l \pmod{m}$.

A prova do Teorema de Dirichlet para todo (a,m) é bastante complicada, pois usa métodos avançados de cálculo, assim não a daremos neste trabalho. Ver por exemplo [RIBENBOIM, 89].

Prova.[RAYES,98] Dos resultados dos lemas (5.2) e (5.3) resta mostrar que existem infinitos primos da forma $p = 4nK + 1$ e $p = 4nK - 1$. Isto segue do teorema 5.6 para $(l,m) = (1, 4n)$ e para $(l, m) = (-1, 4n)$, respectivamente.□

Exemplo(5.3): Considere $T_6(x) = 32\,x^6 - 48\,x^4 + 18x^2 - 1$. Primos da forma $p = 4nK + 1$, inclui $p = 73$, para $K = 3$ e primos da forma $p = 4nK-1$ inclui $p = 23$, para $k = 1$. Temos

$$T_6(x) \equiv 32(x+30)(x+59)(x+16)(x+14)(x+43)(x+57) \pmod{73} \qquad (5.19)$$

$$T_6(x) \equiv 9(x+19)(x+4)(x+10)(x+9)(x+14)(x+13) \pmod{23} \qquad (5.20)$$

As propriedades modulares dos polinômios $U_n(x)$ são similares a estas dos polinômios $T_n(x)$. Observe que

$$\eta_k = \frac{w^k + w^{-k}}{2},\ k = 1, \ldots, n,$$

em que $w = e^{\pi ki/(n+1)}$ é uma $(2n+2)^{th}$ raiz complexa primitiva da unidade, podemos mostrar

Teorema (5.6) Seja $n \geq 2$ inteiro. Para todos os infinitos inteiros positivos K para qual $p = 2(n+1)k \pm 1$ é um número primo, $U_n(x)$ tem n raízes em Z_p.

5.5 - Determinando as Raízes Modulares

Esboçaremos, métodos para encontrar as raízes de um polinômio de Chebyschev num determinado corpo finito Z_p, que contenha todos seus zeros. Construímos algoritmos eficientes que toma como input um inteiro $n > 1$ e um primo $p = 4nK \pm 1$ ($p = 2(n + 1) k \pm 1$) e calculamos todos os zeros de $T_n(x)(U_n(x))$ módulo p. Consideramos primeiro o caso $p = 4nK+1(2(n + 1)K+ 1)$ para algum $K > 0$. Neste caso, o corpo Z_p tem uma $(4n)^{th}((2n + 2)^{th})$ raiz primitiva θ da unidade. É fácil encontrar θ, se primeiro procuramos um elemento primitivo $\beta \in Z_p$. É bem conhecido que β satisfaz $(p-1, \beta) = 1$. Considerando que n e K são conhecidos, podemos escolher β como o primeiro primo ímpar que não divide n ou K ($n+1$ *ou* K). Uma vez que um elemento primitivo β é escolhido, uma $(4n)^{th}$ $((2n + 2)^{th})$ raiz primitiva θ da unidade é obtida fixando

$$\theta = \beta^{(p-1)/4n} \quad (\theta = \beta^{(p-1)/(2n+2)}).$$

As raízes são então prontamente calculadas pela relação $\xi k = (\theta^{2k-1} + \theta^{2k+1})/2$ ($\eta_k = (\theta^k - \theta^{-k})/2$). Formalizamos essas idéias no algoritmo Proots (Fig. 1).

Algoritmo Proots(n,K)

Entrada: Inteiros, n, K, Q = { $p_1 = 3, p_2 = 5, p_3 = 7, p_4 = 11, \ldots$ }

Saída: Raízes de $T_n(x)$ mod $4nK + 1$ [$U_n(x)$ mod $2(n+1)K + 1$]

PRoots-1 $p = 4nK+1$ [$2(n+1)K+1$]

PRoots-2 (find β)

For j = 1 to p-1 do

2.1 β = pj

2.2 if β ∤ n or β ∤ k[β ∤ (n+1) or β ∤ k] then

pare

PRoots-3 $\theta = \beta^{(p-1)/4n}$ $(\theta = \beta^{(p-1)/(2n+2)})$

PRoots-4 for k = 1 to n do
saída $\xi_k = (\theta^{2k-1} + \theta^{2k+1})/2$ $[\eta_k = (\theta^k - \theta^{-k})/2]$

Figura 1: Algoritmo para calcular as raízes de $T_n(x)$ $(U_n(x))$.

O número de passos requeridos pelo algoritmo Proots é limitado pelos primos p_j de Q, que precisam ser testados, que por sua vez são limitados pelo número de primos menores ou iguais a p. Em outras palavras, de acordo com o Teorema do número primo (veja [ANDERSON, 97 pp.120], o algoritmo Proots tem ordem $O(p/\log p)$.

Exemplo (5.4) Considere $T_6(x)$ e $p = 73 = 4 \times 6 \times 3 + 1$. Aqui o primeiro elemento primitivo de Z_p é $\beta = 5$. A $(24)^a$ raiz primitiva da unidade correspondente é $\theta = 5^{72/24} = 5^3 = 52 \pmod{73}$. Os zeros aparecem no exemplo acima. Se tomamos $U_6(x)$ e $p = 29 = 2(6+1)2 + 1$, o primeiro elemento primitivo de Z_p é $\beta = 3$. A $(14)^a$ raiz primitiva da unidade correspondente é $\theta = 3^{28/14} = 3^2 = 9 \pmod{29}$. Os zeros de $U_6(x) \pmod{29}$ são 11, 9, 13, 16, 20 e 18. Consideramos o caso em que $p = 4nK-1$ $(p = 2(n+1)K-1)$, onde o corpo de extensão, $GF(p^2)$ tem uma $(4n)^{th}$ $((2n+2)^{th})$ raiz primitiva da unidade θ, que desejamos encontra-la. A Lei da *Reciprocidade Quadrática* estabelece que: se -1 não é um quadrado módulo p, então o polinômio $x^2 + 1$ é irredutível em Z_p. Podemos então considerar $GF(p^2)$ como os inteiros Gaussianos, com aritmética feita módulo p. Para p pequeno, é razoável encontrar uma $(4n)^{th}$ $((2n + 2)^{th})$ raiz primitiva da unidade θ por tentativa e erro, obtendo primeiro um elemento primitivo em $Z_p \times iZ_p$. Uma procura mais eficiente é usar o resultado do lema (5.3). Encontramos soluções $c, d \in Z_p$ para a equação $c^2 + d^2 = 1$. Calcule a ordem t do elemento $\beta = c + id \in Z_p \times iZ_p$. Note t sempre divide $p+1$, pelo lema (5.3). Se $4n$ divide t ($2n + 2$ divide t), então levamos $\theta = \beta^{t/4n}$ $(\theta = \beta^{t/(2n+2)})$ como nossa $(4n)^{th}$ $((2n+2)^{th})$ raiz primitiva da unidade. Repetimos a procura até que $4n$ divida t ($2n + 2$ divida t). Como $p+1$ divide $p^2 - 1$, sabemos que existem elementos de ordem $p+1$ em $Z_p \times iZ_p$ e esta procura terminará. Este algoritmo eficiente é mostrado na figura 2.

Algoritmo MRoots(n,K)

Entrada: Inteiros, n,K

Saída: Raízes de $T_n(x) \bmod 4nK-1$ $[U_n(x) \bmod 2(n+1)k-1]$

MRoots-1 $p = 4nK-1$ $[2(n+1)K-1]$

MRoots-2 for j = 1 to p-1 do
for k = 1 to p-1 do
$a = j^2 + k^2 (\text{mod } p)$
if a = 1 then
{ t = order ($\beta = j + k \times i \bmod p$)
if (4n(2n+2)\t) then goto(step 3)}
done
done

MRoots-3 $\theta = \beta^{t/4n}$ $(\theta = \beta^{t/(2n+2)})$

Mroots-4 for k = 1 to n do saída $\xi_k = (\theta^{2k-1} + \theta^{2k+1})/2$ $[\eta_k = (\theta^k - \theta^{-k})/2]$

Figura 2 : Outro algoritmo para raízes de $T_n(x)$ $(U_n(x))$

Procurar raízes modulares num dado corpo é um problema que consome muito tempo, porque a cardinalidade do corpo finito é p^2. Mas não existe nenhum algoritmo conhecido eficiente, para achar um elemento primitivo no corpo $Z_p \times iZ_p$. Uma estimativa muito grosseira da complexidade do algoritmo MRoots é $O(p^3)$ que possui a mesma ordem de um procedimento por tentativa e erro. Claramente esta complexidade no pior caso é improvável e uma análise da complexidade mais detalhada do algoritmo valerá a pena.

Exemplo(5.5) Sejam $U_3(x)$ e $p = 23 = 2(3+1)3-1$. Soluções (c,d) para $c^2 + d^2 = 1 \pmod p$ incluem (4,10), (8,11), (9,9), (10,19),(11,15). As ordens respectivas dos elementos correspondentes são 24, 12, 8, 24, 3 e podemos fazer $\theta = (4 + 10i)^{24/8} = 14 + 9i$ como a $(8)^a$ raiz primitiva da unidade. As raízes correspondentes são 14, 0, 9.

6 – Polinômios de Chebyshev e Primalidade de Inteiros

Nesse capítulo apresentaremos a relação entre primalidade de números inteiros e os polinômios de Chebyshev, mostrando resultados recentemente descobertos. Daremos também o algoritmo usado na simulação numérica de um desses resultados, assim como os resultados obtidos na pesquisa.

6.1 – Primalidade de inteiros e a irredutibilidade dos polinômios de Chebyshev

Apresentaremos a relação entre a primalidade de qualquer inteiro n e a irredutibilidade dos polinômios de Chebyshev do primeiro tipo $T_n(x)$. Baseado nesta relação, os critérios de primalidade de inteiros são desenvolvidos. Nesta seção, sem perda de generalidade, considere n como sendo um inteiro ímpar e os polinômios de Chebyshev de grau n, como sendo $T_n(x) = \sum_{k=0}^{n} t_k x^k$. Existem muitas fórmulas fechadas e relações de recorrências para os coeficientes t_k de $T_n(x)$. A fórmula seguinte é devido a [SNYDER, 66, p.14]. Seja

$$T_m^k = (-1)^k 2^{m-1} \frac{m+2k}{m+k} \binom{m+k}{k}, \tag{6.1}$$

então para $n = 2m + 1$, temos

$$T_n(x) = \sum_{k=0}^{m} T_{2k+1}^{m-k} x^{2k+1}. \tag{6.2}$$

Lema (6.1): Seja n um primo ímpar. O polinômio $T_n(x) / x$ é irredutível.

Prova:[RAYES, 99] Se escrevemos $n = 2m + 1$, o coeficiente T_{2k+1}^{m-k} de x^{2k+1} em $T_n(x)$ é dado por

$$T_{2k+1}^{m-k} = (-1)^{m-k} 2^{2k} \frac{2m+1}{m+k+1} \binom{m+k+1}{m-k}.$$

Pode ser visto por inspeção, que o coeficiente principal $T_n^0 = 2^{n-1}$, o coeficiente independente $T_1^m = (-1)^m n$ e os coeficientes restantes são todos divisíveis por n. A irredutibilidade de $T_n(x)$ / x segue pelo critério de Eisenstein, que é dado abaixo.□

Critério de Eisenstein: Se $f = \sum_{k=0}^{r} c_k x^k$ é um polinômio de grau $r > 0$, com coeficientes num anel fatorial A e se existe um elemento irredutível p em A tal que $p^2 \nmid c_0$, $p \nmid c_r$ e $p \mid c_k$ para $k = 0, 1, \ldots, r-1$, então o polinômio f é irredutível em $K[x]$, em que K é o corpo de frações de A.

Lema (6.2): (Teorema) Seja $p = 2h + 1$ um divisor primo de $n = 2m + 1$. Então n não divide o coeficiente T_p^{m-h} de x^p em $T_n(x)$.

Prova:[RAYES, 99] Uma manipulação da fórmula fechada (6.1) para T_p^{m-h}, permite obter:

$$T_p^{m-h} = (-1)^{m-h} 2^{p-1} \frac{p+2(m-h)}{p+m-h} \binom{p+m-h}{m-h}$$

$$= (-1)^{m-h} 2^{p-1} \frac{p+2m-2h}{p+m-h} \binom{p+m-h}{p+m-h-(m-h)}$$

sabendo que $\binom{a}{b} = \binom{a}{a-b}$, $2h = p-1$ e $2m = n-1$, temos

$$T_p^{m-h} = (-1)^{m-h} 2^{p-1} \frac{p+n-1-p+1}{p+m-h} \binom{p+m-h}{p}$$

$$= (-1)^{m-h} 2^{p-1} \frac{p+(n-p)}{p+m-h} \binom{p+m-h}{p}.$$

Usando a propriedade $\binom{a}{b} = \frac{a}{b}\binom{a-1}{b-1}$, temos

$$T_p^{m-h} = (-1)^{m-h} 2^{p-1} \frac{n(p+m-h)}{(p+m-h)p} \binom{p+m-h-1}{p-1}$$

$$= (-1)^{m-h} 2^{p-1} \frac{n}{p} \binom{p+m-h-1}{p-1}.$$

Sabemos que p, não divide o coeficiente binomial $\binom{p+m-h-1}{p-1}$, porque existem $p-1$ fatores consecutivos no seu numerador começando com $m-h+p-1$. Daí n não divide T_p^{m-h} como estabelecido.□

Estamos prontos para o seguinte teorema:

Teorema (6.1): Seja n um inteiro positivo ímpar. Então n é primo se e somente se, $T_n(x)/x$ for irredutível sobre os inteiros.

Prova:[RAYES, 99] Se n é primo, então fica claro pelo Lema (6.1) que $T_n(x)/x$ satisfaz o critério de irredutibilidade Eisenstein. Suponha que $T_n(x)/x$ seja irredutível em $Z[x]$. Segue que $T_n(x)$ tem exatamente dois fatores irredutíveis, segundo o corolário (5.2) o número de fatores irredutíveis de $T_n(x)$ é igual ao número de divisores ímpares de n. Daí, n é primo.□

O Teorema (6.1) mostra a equivalência entre a primalidade de um inteiro ímpar n e a irredutibilidade dos polinômios de Chebyschev $T_n(x)$ dividido por x. Esse resultado, na forma como está estabelecido, pode não ser prático, porque o cálculo e o armazenamento dos coeficientes de $T_n(x)$ é proibitivo para valores grandes de n. O seguinte teorema minimiza um pouco o problema.

Teorema (6.2): Um inteiro ímpar $n = 2m + 1 > 1$ é primo se e somente se,

$$T_n(x) \equiv x^n \ (mod\ n).$$

Prova: [RAYES, 99] Escrevemos $T_n(x) = \sum_{k=0}^{n} t_k x^k$. Se n for primo, então como a prova do Lema (6.1) indica, $T_n(x)/x$ satisfaz o teste de irredutibilidade de Eisenstein e $a_k \equiv 0 \ (mod\ n)$ para $k = 0, 1, 2, ..., n-1$. Para $k = n$, temos $t_n^0 = 2^{n-1} \equiv 1 (mod\ n)$, pelo teorema de Fermat. Por outro lado, suponha que n é composto. Seja $p = 2h + 1$ um primo que divide n. O Lema (6.2) mostra que $t_p = T_p^{m-h}$ não é divisível por n, o que implica $T_p(x) \not\equiv x^p \ (mod\ p)$. □

Esse critério é aparentemente mais prático que o teorema (6.1), uma vez que requer a construção um polinômio de Chebyshev de grau n *módulo* n. Para esta construção, a técnica do divide e conquista pode ser usada, podendo ser deduzida da equação (5.5).

$$T_{2m+1}(x) = 2\, T_{m+1}(x)\, T_m(x) - T_1(x) \tag{6.3}$$

Contudo, deve ser notado que o critério não é um teste de primalidade eficiente, levando em consideração que o custo é dominado pela multiplicação polinomial $T_{m+1}(x)\ T_m(x)$, que é dependente do número de coeficientes não nulos. Acontece que, a grosso modo, metade dos coeficientes de $T_{m+1}(x)$ e $T_m(x)$ são não nulos uma vez que não existe cancelamento módulo n.

Aplicando o teorema de Fermat e o teorema (6.2), podemos estabelecer

Teorema (6.3): Se um inteiro $n > 1$ é primo, então $T_n(a) \equiv a \ (mod\ n)$ para todo inteiro a, $1 \leq a \leq n-1$.

Para computar $T_n(x)$ em um ponto a, poderemos usar a relação de recorrência definida por

$$\begin{aligned} T_0(a) &= 1 \\ T_1(a) &= a \\ T_k(a) &= 2a\, T_{k-1}(a) - T_{k-2}(a) \quad k = 2, 3, \ldots \end{aligned} \tag{6.4}$$

que possui a fórmula fechada

$$T_k(a) = \frac{1}{2}\left[\left(a+\sqrt{a^2-1}\right)^k + \left(a-\sqrt{a^2-1}\right)^k\right]. \qquad (6.5)$$

Note que, a seqüência de Lucas $V_n(a,b) = \alpha^n + \beta^n$ para $n \geq 0$, em que α e β são as raízes do polinômio $x^2 - ax + b$ [Ribenboim, 89] satisfaz a propriedade:

$$V_k(2a, 1) = 2aV_{k-1} - V_{k-2} = 2\,T_k(a), \quad k \geq 2 \qquad (6.6)$$

Daí, que todas as propriedades das seqüências de Lucas, particularmente sua relação com primalidade, podem também ser satisfeitas pela seqüência de Chebyshev $T_k(a)$ definida em (6.4).

Alternativamente, se $T_n(a)$ pode ser calculado usando a relação (6.3). Isto pode ser feito usando apenas $O(\log n)$ operações em Z_n. Num certo sentido, o teorema (6.3) pode ser visto como uma generalização do pequeno teorema de Fermat. Mais exatamente, para n primo, não apenas $a^n \equiv a \pmod n$, mas $T_n(a) \equiv a \pmod n$. Note também, que se a recíproca do teorema (6.3) é verdadeira, um teste de primalidade determinístico eficiente pode ser desenvolvido. Seguindo essas similaridades com o pequeno teorema de Fermat, podemos chamar um inteiro n como um pseudoprimo de Chebyshev na base a, se n é composto e $T_n(a) \equiv a \pmod n$.

Baseado nesses fatos, também definimos um pseudoprimo forte que chamaremos de número de Chebyshev :

Definição(6.1): Um inteiro composto positivo n é um número de Chebyshev, se $T_n(a) \equiv a$ para todo a, $1 \leq a < n$.

A seguir apresentamos o algoritmo desenvolvido em nossa pesquisa, como também a sua complexidade. O mesmo se fundamenta no resultado do teorema 6.3.

6.2 – O algoritmo usado na pesquisa

Dos critérios de primalidade relatados acima, desenvolvemos um algoritmo que usa a relação de recorrência 5.3 numa tentativa de provar a recíproca do resultado do teorema 6.3.

Algoritmo Polch 1

Entrada: $n > 2$ (número inteiro positivo ímpar)
Saída: "n é primo" ou "n é composto"

Passo 1: Entre com o valor de n inteiro positivo ímpar;
Passo 2: if $(n > 2)$ then
do a = 1, n-1
$T_0(a) = 1$
$T_1(a) = a$
do i = 1, n-1
$T_i(a) = (2i\ T_{i-1}(a) - T_{i-2}(a)) \bmod n$
end do
end do
end if
Passo 3: if ($T_i(a) = a$) then
" n é primo "
else
"n é composto"
end if
end algoritmo Polch 1

Análise da complexidade – calculamos a complexidade desse algoritmo analisando apenas o passo 2, pois é nele que se encontram o número de operações exigidas para obtermos o resultado final do algoritmo.

O custo desse teste é o custo da operação $T_n(a)(mod\ n)$. O número de operações (multiplicação/adição) para essa operação é $O(n)$, sem considerarmos o número de dígitos,

se a e b tem k dígitos, então o produto $a.b$ tem $O(k^2)$ operações. Assim, como há $O(\log n)$ operações cada uma envolvendo número com $\log n$ dígitos, então a ordem de complexidade desse algoritmo é $O(n((\log n)^2)$para cada a, como temos um total de a = n, segue que a complexidade desse algoritmo é $O(n^2(\log n)^2)$*operações.*

Para n primo o resultado desse algoritmo sempre estará correto, i.e, $T_i(a) \equiv a \pmod n$, porém fizemos uma simulação numérica implementando esse algoritmo na linguagem de programação FORTRAN 90 (anexo 9.2) , para responder a seguinte questão: para n composto $T_n(a) \equiv a \pmod n$, para todo a?, i.e, existe algum n composto tal que $T_n(a) \equiv a \pmod n$ para todo a, $1 \leq a \leq n-1$? Na tentativa de obtermos uma resposta negativa à essa questão, pois assim a recíproca do teorema 6.3 será verdadeira, conduzindo-nos à um novo teste de primalidade determinístico. A seção seguinte relata os resultados obtidos em nossa simulação numérica .

6.3 – Resultados obtidos na pesquisa

Até o momento não encontramos números de Chebyshev, isso significa que, como vimos anteriormente, não encontramos nenhum número composto n ($n < 1{,}9 \times 10^4$) que passasse no teste para todos os valores de a, $1 \leq a \leq n-1$, e isso foi o fato mais importante de nossa pesquisa, pois garante a recíproca do teorema 6.3 para os valores analisados. Todos aqueles números declarados primos (Total = 2131) em nossa simulação, foram confirmados primos no Maple.

A tabela 1 (é uma síntese do anexo 9.1) mostra na sua primeira coluna as duas primeiras testemunhas da composição de n, i.e, mostra os dois primeiros valores de a que declaram que n é composto; a segunda coluna apresenta a quantidade de valores de inteiros positivos ímpares e compostos n correspondentes às testemunhas da primeira coluna; e a terceira coluna, mostra a porcentagem que a quantidade da segunda coluna representa do total de inteiros compostos e ímpares n pesquisados.

Tabela 1 – Percentagem de testemunhas

Testemunhas da composição	Quantidade de *n*	%
2,3	7249	98,42
2,4	51	0,69
2,5	8	0,10
2,6	1	0,01
2,7	1	0,01
3,4	45	0.62
3,5	2	0,02
3,6	1	0,01
4,5	3	0,04
4,6	1	0,01
4,8	1	0,01
5,6	1	0,01

Observe que a maioria absoluta dos número inteiros compostos n pesquisados, a composição deles é anunciada para valores de $a = 2$ ou 3. Também é observado que todos os números compostos, em nossa pesquisa, a sua composição é declarada para valores pequenos de a. Até o momento, nas duas primeiras testemunhas o maior valor que apareceu foi 8.

Números de Carmichael conhecidos, como 561 que é o menor número de Carmichael, sua composição é declarada imediatamente, isso significa dizer que, eles são declarados compostos, para valores pequenos de a.

O menor pseudoprimo na base 2 é 209, isso significa dizer que, ele é o primeiro número composto, para o qual $a = 2$ não declara sua composição.

O 5719 é o primeiro número composto que não apresenta $a = 2$ *ou* 3, como testemunha da composição. Sua primeira testemunha é $a = 4$, que também é um valor pequeno.

A densidade e a distribuição dos inteiros a tais que $T_n(a) \equiv a \ (mod\ n)$, para todos os n compostos pesquisados, foi feita porém mostrar aqui necessitaria de muito espaço, motivo esse que nos conduz a apresentar apenas os problemas encontrados, i.e, os valores de n considerados ruins em nossa pesquisa. Problemas esses considerados poucos, visto a quantidade de números pesquisados. Os números que não aparecem na tabela a seguir foram considerados óti-

mos em nosso trabalho, pois a quantidade de falsas testemunhas é pequena, isso significa que, a composição desses n é dada por uma quantia superior a 75% de testemunhas. Analisando os nossos arquivos de distribuição das testemunhas da composição, podemos declarar que a maioria dos números compostos pesquisados, apresentam porcentagem de falsas testemunhas inferior a 2%.

A seguir apresentamos a tabela 2 que mostra os pontos considerados críticos em nossa pesquisa. A primeira coluna da tabela apresenta os valores de n inteiro positivo composto ímpar que, comparados ao teste de primalidade de Miller-Rabin, deram problema (A quantidade de falsas testemunhas é superior a 25%.); a segunda coluna apresenta a quantidade de a, $1 \leq a \leq n-1$ para os quais $T_n(a) = a$, i.e, quantidade de a, que declara n como sendo primo (o que não é verdade); a terceira coluna apresenta as duas primeiras testemunhas da composição de n, i.e, os dois primeiros valores de a que declaram que n é composto. Na última coluna apresentamos a porcentagem de erro, ou seja, a porcentagem dos pseudoprimos nas diferentes bases, para cada n.

Tabela 2 – Pontos críticos

n composto	**Total de "a" que declaram n como primo**	**As duas primeiras testemunhas da composição de n**	**Representação em porcentagem (%)**
15	8	2, 3	53,33
21	9	2, 3	42,85
33	9	2, 3	27,27
35	25	2, 5	71,42
55	25	2, 3	45,45
65	25	2, 3	38,46
77	25	2, 3	32,46
85	25	2, 3	29,41
91	25	2, 3	27,47
95	25	2, 3	26,31
105	45	2, 3	42,85
119	49	2, 4	41,17
143	49	2, 3	34,26
161	49	2, 3	30,43
195	81	2, 3	41,53
209	81	3, 4	38,75

231	105	3, 4	45,45
255	81	2, 3	31,76
319	80	2, 3	25,39
323	121	2,3	37,46
377	121	2, 3	32,09
385	245	2, 4	63,63
399	165	3, 4	41,35
455	245	3, 4	53,84
* 561	189	2, 3	33,68
595	275	2, 3	46,21
665	385	2, 3	57,89
715	275	2, 3	38,46
741	297	2, 5	40,08
899	289	2, 4	32,14
935	454	2, 4	48,66
1001	315	2, 3	31,46
1045	385	2, 3	36,84
* 1105	715	2, 3	64,70
1295	665	3, 4	51,35
1443	567	2, 3	39,29
1495	425	2,3	28,42
1595	595	2, 3	37,30
* 1729	735	3, 4	42,51
1763	529	2, 3	30,00
2001	585	2, 4	29,23
2015	1235	3, 6	61,29
2345	735	3, 4	31,34
2431	765	2, 3	31,46
* 2465	1445	2, 3	58,62
2639	833	3, 4	31,56
2703	729	2, 3	26,97
2737	1547	2, 3	56,52
2849	1449	2, 3	50,85
2915	1015	2, 3	34,81
3059	1614	2, 4	52,76
3289	1859	2, 3	56,52
3599	961	2, 3	26,70
3655	1495	2, 3	40,90
3689	1729	2, 4	46,86
4081	1309	2, 3	32,07
4199	1183	2, 4	28,17
4355	2275	2, 3	52,53

* Número de Carmichael.

4465	1375	2, 3	30,79
4879	2737	2, 4	56,09
4991	2093	2, 3	41,93
5183	1369	2, 3	26,41
5291	2717	3, 4	51,35
5719	2275	4, 5	39,77
6061	3289	5, 6	54,26
6479	4807	2, 5	74,19
6545	1925	2, 3	29,41
* 6601	3703	2, 4	56,09
6721	3575	2, 3	53,19
7055	3655	2, 7	51,80
8569	4785	3, 4	55,84
8855	3185	2, 3	35,96
* 8911	3675	2, 3	41,24
9361	2717	2, 3	29,02
9503	2975	3, 4	31,30
10403	2809	2, 5	27,00
10439	2849	3, 4	27,29
10465	3185	2, 3	30,43
* 10585	3145	2, 3	29,71
11285	5075	2, 4	44,97
11305	5005	2, 3	44,27
11395	4495	4, 5	39,44
11663	3025	2, 3	25,93
11935	3325	2, 3	27,85
11951	4845	3, 4	40,54
12121	3059	3, 4	25,23
13079	4300	2, 4	32,87
13735	4625	3, 4	33,66
14705	3995	2, 3	27,16
14839	4797	3, 5	32,32
15457	5525	2, 3	35,73
15841	8029	4,8	50,67
16211	6279	2,3	38,72
16835	4375	2,3	25,98
17081	4389	2,3	25,68
17119	9367	4,5	54,71
17423	5159	2,3	29,60
17641	5239	2,3	29,69
18095	6124	2,3	33,84
18239	4990	3,4	27,35
18241	6324	2,5	34,66

Vimos que embora a tabela acima mostre, que todos esses valores de n apresentam uma taxa de erro maior que o teste de Miller-Rabin (25 % de falsos testemunhas), um ponto positivo pode ser observado. Todos esses n, são declarados compostos para valores pequenos de a. Exemplo, o número 6479, apresenta uma taxa de erro muito alta (até o momento, a maior 74,19 %), mas é declarado sua composição para $a = 2$. Os números de Carmichael, que conhecíamos, foram declarados compostos, embora exista uma taxa meio grande de erros, como exemplo citamos o número 1105 que apresenta a maior para números de Carmichael, 64,61% .

É interessante notar que, fazendo um estudo da distribuição dos problemas, estes se distribuem de uma forma não uniforme, observe a tabela 3 abaixo.

Tabela 3 – Distribuição dos problemas

Intervalo de n inteiro ímpar composto	**Quantidade de problemas**
1 à 1000	31
1001 à 2000	9
2001 à 3000	10
3001 à 4000	5
4001 à 5000	6
5001 à 6000	3
6001 à 7000	5
7001 à 8000	1
8001 à 9000	3
9001 à 10000	2
10001 à 11000	4
11001 à 12000	6
12001 à 13000	1
13001 à 14000	2
14001 à 15000	2
15001 à 16000	2

16001 à 17000	2
17001 à 18000	4
18001 à 19000	3

Foi utilizado nessa pesquisa um micro Compaq 4550 233MHZ com 3,73GB de HD e 48 MB de RAM.

O tempo de execução do algoritmo, nos diferentes intervalos de n, pode ser encontrado no anexo 9.3, porém nem todas as vezes foi possível registrá-lo, por motivo de falta de energia ou pane no computador, .

7 – CONCLUSÃO

O objetivo central desse trabalho era, através de simulação numérica, provar a recíproca do seguinte resultado: "se n é primo, então $T_n(a) \equiv a \ (mod\ n)$, para todo a, $1 \leq a \leq n-1$". Tal recíproca é que, para n composto, essa congruência não é válida para todo a, significa dizer que, " se n é composto, então $T_n(a) \not\equiv a \ (mod\ n)$, para algum a, $1 \leq a \leq n-1$. Para isso usamos a fórmula de recorrência dos polinômios de Chebyshev, implementado-a na linguagem FORTRAN 90, usando precisão dupla, numa tentativa de obtermos uma resposta concreta para tal objetivo.

Os valores de n pesquisados são menores que 19000, porém já se pode conjecturar: " Se n é composto, então existirá um a, $1 \leq a \leq n-1$, tal que $T_n(a) \not\equiv a \ (mod\ n)$", pois para esses valores não encontramos nenhum número inteiro ímpar maior que zero que invalidasse esse resultado.

Dos resultados encontrados na pesquisa, fizemos comparações a resultados de testes de primalidade existentes na literatura, especificamente o teste de Miller – Rabin, citado no capítulo 4, que apresenta uma performance reconhecida por estudiosos da área, i.e, apresenta uma margem de erros pequena (25 % de falsas testemunhas). Dessas comparações encontramos alguns pontos considerados críticos que são: o número 6479, que apresenta muitas falsas testemunhas (até o momento a maior: 74,19 %), mas é declarado sua composição para a = 2 e isso é um ponto positivo do teste em potencial que estamos sugerindo em nossa pesquisa. De fato pode ser observado que em mais de 98,42 % dos

números inteiros ímpares compostos pesquisados, sua composição é declarada para valores muito pequenos de a: a = 2 ou 3.

Números de Carmichael, que conhecíamos, também foram declarados compostos para valores pequenos de *a*, embora para alguns também exista uma margem grande de erros, como citamos o número 1105, que apresenta a maior para número de Carmichael, igual a 64,61 % de falsas testemunhas.

Outro ponto importante de nosso trabalho é que os dados obtidos estão armazenados (de forma eletrônica e impressa), de modo que trabalhos futuros poderão se valer das informações neles contidos. É nossa idéia estudar a distribuição das (falsas) testemunhas, de modo a jogar luz nesse problema. Será que a distribuição é uniforme ?

Evidentemente, o objetivo futuro mais importante é a prova da recíproca desse resultado (ou a refutação através de um exemplo). Entretanto, mesmo que esse objetivo esteja fora do nosso alcance atual, acreditamos que se forem seguidos os passos Miller, será possível definir um teste de modo a detectar pseudoprimos fortes. Isso, aliado a uma análise probabilística, seguindo as pegadas de Rabin, podem levar a um eficiente teste de primalidade probabilístico.

Em um futuro imediato, acreditamos que poderíamos melhorar a eficiência desse teste que utilizamos para a simulação, através de outros resultados. Como exemplo, podemos citar a equação (6.3) $T_{2m+1}(x) = 2T_{m+1}(x) - T_1(x)$, que requer a construção de um polinômio de Chebyshev de grau *n* módulo *n*. Para essa construção, poderá ser utilizado a técnica do divide e conquista, que deverá reduzir o número de operações para O(log n). Também poderá ser utilizado a mesma relação de recorrência utilizada nesse trabalho, fazendo uso da fórmula fechada (6.5) $T_k(a) = \frac{1}{2}\left[\left(a+\sqrt{a^2-1}\right)^k + \left(a-\sqrt{a^2-1}\right)^k\right]$. Donde fizemos a relação com as seqüências de Lucas , falando da propriedade, $V_k(2\ a,\ 1\ ) = 2T_k(a)$, em que $V_n(a,b) = \alpha^n + \beta^n$ para $n > 0$ é a seqüência de Lucas com α e β sendo as raízes do polinômio $x^2 - ax + b$. Independente do algoritmo usado para o cálculo de $T_n(a)$, é

imprescindível o uso de uma aritmética de precisão múltipla (não só dupla) para valores grandes de n.

8 - Bibliografia

[ALFORD, 94] Alford, W. R., Granville, A. and C. Pomerance. "There are infinitely many Carmichael numbers."Annals of Math, 140 (1994, 703-732).

[ANDERSON, 97] Anderson, James Andrew and Bell, James Milton. *Number Theory, with applications.* Prentice-Hall, 1997.

[BRESSOUD, 98] Bressoud, David M. *Factorization and Primality Testing.* Springer-Verlag, 1998

[COHEN,95] Cohen, H., *A Course in Computational Algebraic Number Theory.* Springer-Verlag, Germany, 1995.

[CONDE,75] Almeida, Luiz Ignácio Pio. *Elementos de Análise Numérica.* Tradução: Ed. Globo, 1975. (Traduzido de *Elementary Numerical Analisis, an algorithmic approach* - S. D. Conde- MacGaw-hill, 1965) .

[DAMGARD,93] Damgard, Ivan, Landrock, Peter and Pomerance, Carl. "Average Case Error Estimates for the Strong Probable Prime Test." American Mathematical Society, 1993, pp.177-195.

[FOX, 68] Fox, L. and Parker, I.B. *Chebyshev Polynomials in Numerical Analysis*, Oxford University Press, 1968.

[GIBLIN,93] Giblin, Peter. *Primes and Programming. An Introduction to Number Theory with Computing.* Cambridge University Press, 1993.

[YAN,96] Yan, Song Y. *Perfect, Amicable and Sociable Numbers. A computational Approach.* Word Scientific Publishing Co. Pte. Ltd. 1996.

[LEHMER, 33] Lehmer, D. H. "A note on trigonometric algebraic numbers", American Mathematical Monthly 40, 1933, pp. 165-166.

[LIDL, 94] Lidl, Rudolf and Niederreiter, Harald. *Introduction to finite fields and their applications.* Revised Edition. Cambridge. 1994.

[KOBLITZ, 94] Koblitz, Neal. *A Course in Number Theory and Cryptography.* Second Edition. Springer-Verlag. 1994

[KNUTH, 98] Knuth, Donald E. *The Art of Computer Programming*, Vol.2. Addison Wesley, 1998.

[RABIN,80] Rabin, Michael O. " Probabilistic Algorithm for testing Primality." Academic Press, Inc. 1980, pp.128-138.

[RAYES, 98] Rayes, Mohamed O., Trevisan, Vilmar and Wang, Paul S., " Factorization of Chebyshev Polynomials". Tecnical Report ICM – 199802 – 0001. Endereço na web: http://horse.mcs.kent.edu/icm/index.html.

[RAYES, 99] Rayes, Mohamed O., Trevisan, Vilmar and Wang, Paul S., " Chebyshev Polynomials and Primality Tests." Tecnical Report ICM – 199801 – 0002. Endereço na web: http://horse.mcs.kent.edu/icm/index.html.

[RIBENBOIM, 89] Ribenboim, Paulo. *The Book of Prime Number Records*, Second Edition, Springer-Verlag, 1989.

[RIVLIN, 74] Rivlin,T.J. *The Chebyshev Polynomials.* Wiley-Interscience, 1974.

[ROSEN, 93] Rosen, Kenneth H. *Elementary number theory and its applications.* 3rd ed. AT&Bell Laboratories , 1993.

[SANTOS, 98] Santos, José Plínio de Oliveira. *Introdução à Teoria dos Números.* Rio de Janeiro, Instituto de Matemática Pura e Aplicada, CNPq, 1998.

[SCHROEDER,86] Schroeder, M.R. *Number Theory in Science and Communication: With applications in Cryptography, Physics, Digital Information, Computing and Self Similarity.* Second Enlarged Edition, Springer-Verlag, 1986.

[SILVERMAN,97] Silverman, Joseph H. *A Friendly Introduction to Number Theory.* Prentice-Hall, 1997.

[SOLOVAY, 77] Solovay, R. and Strassem, V., "A fast Monte-Carlo test for primality", SIAM J. Comput. 6(1977), 84-85.]

[SNYDER,66] Snyder, M.A., *Chebyshev Methods in numerical Approximation*, Prentice-Hall, N.J. 1966.

GLOSSÁRIO DE SÍMBOLOS

$T_n(x)$	é o n-ésimo polinômio de Chebyshev de 1° tipo.
$T_n(a)$	$T_n(x)$ em um ponto a.
(a, b)	mdc(a, b)
$a \mid b$	a divide b.
$a \nmid b$	a não divide b.
$a \equiv b \ (mod\ m)$	a é congruente a b módulo m se $m \mid (a - b)$.
$a \not\equiv b \ (mod\ m)$	a não é congruente a b módulo m.
a^*	inverso de a módulo m.
$\left(\frac{a}{p}\right)$	símbolo de Legendre.
$\left(\frac{a}{n}\right)$	símbolo de Jacobi.
$\phi(m)$	função de Euler.
$n!$	fatorial de n.
O(n)	ordem da complexidade de um algoritmo.
$U_k(a,b)$ e $V_k(a,b)$	seqüências de Lucas associadas ao par (a,b).
$\binom{n}{p} = \frac{n!}{p!(n-p)!}$	para $n \geq p$ e $n, p \in$ N, chama-se número binomial.
D	discriminante da equação $x^2 - ax + b = 0$.
α, β	raízes da equação $x^2 - ax + b = 0$.
$\lambda_{\alpha,\beta}(n)$	função de Carmichael
$\psi(p)$	$p - \left(\frac{D}{p}\right)$.
$\rho(n) = \rho(n, U)$	o menor $r \geq 1$ tal que $\rho(n)$ divide U_r.
L_k	seqüência de Lucas-Lehmer.
M_n	primos de Mersenne.
$ord_m a$	ordem de $a \ mod\ m$.
$ind_r a$	o expoente de a na base $r \ mod\ m$.
ξ_k	raízes de $T_n(x)$.
$U_n(x)$	é o n-ésimo polinômio de Chebyshev de 2° tipo.
η_k	raízes de $U_n(x)$.

ÍNDICE REMISSIVO

9 – ANEXOS

Anexo 9.1 – Tabela de todos os valores de *n* inteiro positivos ímpares pesquisados

n	Primos	Compostos	Total	Testemunhas da composição
9 à 33	7	6	13	2,3
35	-	1	1	2,5
37 à 167	28	38	66	2,3
169	-	1	1	2,4
171 à 207	7	12	19	2,3
209	-	1	1	3,4
211 à 229	5	5	10	2,3
231	-	1	1	3,4
233 à 383	26	50	76	2,3
385	-	1	1	2,4
387 à 397	2	4	6	2,3
399	-	1	1	3,4
401 à 453	9	18	27	2,3
455	-	1	1	3,4
457 à 739	44	98	142	2,3
741	-	1	1	2,5
743 à 777	6	12	18	2,3
779	-	1	1	2,4
781 à 897	17	42	59	2,3
899	-	1	1	2,4
901 à 903	-	2	2	3,4
905 à 921	3	6	9	2,3
923	-	1	1	3,4
925 à 933	1	4	5	2,3
935	-	1	1	2,4
937 à 959	4	8	12	2,3
961	-	1	1	2,4
963 À 987	4	9	13	2,3
989	-	1	1	3,4
991 À 1103	19	38	57	2,3
1105	-	1	1	2,5
1107 À 1119	2	5	7	2,3
1121	-	1	1	2,4
1123 à 1187	8	25	33	2,3
1189	-	1	1	2,4
1191 à 1293	15	37	52	2,3

1295	-	1	1	3,4
1297 à 1441	18	55	73	2,3
1443	-	1	1	2,6
1445 à 1477	5	12	17	2,3
1479	-	1	1	2,4
1481 à 1727	36	88	124	2,3
1729	-	1	1	3,4
1731 à 1853	14	48	62	2,3
1855	-	1	1	3,4
1857 à 1999	20	52	72	2,3
2001	-	1	1	2,4
2003 à 2013	2	4	6	2,3
2015	-	1	1	3,6
2017 à 2209	24	73	97	2,3
2211	-	1	1	3,4
2213 à 2417	30	73	103	2,3
2419	-	1	1	2,4
2421 à 2553	15	52	67	2,3
2555	-	1	1	2,4
2557 à 2637	8	33	41	2,3
2639	-	1	1	3,4
2641 à 2699	11	19	30	2,3
2701	-	1	1	3,4
2703 à 2793	13	33	46	2,3
2795	-	1	1	3,4
2797 à 2909	15	42	57	2,3
2911	-	1	1	3,4
2913	-	1	1	2,3
2915	-	1	1	2,4
2917 à 3005	10	35	45	2,3
3007	-	1	1	3,4
3009 à 3057	6	19	25	2,3
3059	-	1	1	2,4
3061 à 3105	5	18	23	2,3
3107	-	1	1	2,4
3109 à 3199	10	36	46	2,3
3201	-	1	1	3,4
3203 à 3381	24	66	90	2,3
3383	-	1	1	2,4
3385 à 3437	5	22	27	2,3
3439	-	1	1	3,4
3441 à 3533	13	34	47	2,3
3535	-	1	1	3,5
3537 à 3603	9	25	34	2,3

3605	-	1	1	2,5
3607 à 3687	11	30	41	2,3
3689	-	1	1	2,4
3691 à 3739	8	17	25	2,3
3741	-	1	1	2,4
3743 à 3779	4	15	19	2,3
3781	-	1	1	2,5
3783 à 3799	2	7	9	2,3
3801	-	1	1	3,4
3803 à 3825	3	9	12	2,3
3827	-	1	1	2,4
3829 à 4197	43	142	185	2,3
4199	-	1	1	2,4
4201 à 4793	71	226	297	2,3
4795	-	1	1	2,4
4797 à 4821	4	9	13	2,3
4823	-	1	1	3,4
4825 à 4877	4	23	27	2,3
4879	-	1	1	2,4
4881 à 4899	1	9	10	2,3
4901	-	1	1	2,4
4903 à 5289	47	147	194	2,3
5291	-	1	1	3,4
5293 à 5717	52	161	213	2,3
5719	-	1	1	4,5
5721 à 6059	37	133	170	2,3
6061	-	1	1	5,6
6063 à 6081	3	7	10	2,3
6083	-	1	1	2,4
6085 à 6213	15	50	65	2,3
6215	-	1	1	2,4
6217 à 6263	6	18	24	2,3
6265	-	1	1	2,4
6267 à 6439	22	65	87	2,3
6441	-	1	1	2,4
6443 à 6477	4	14	18	2,3
6479	-	1	1	2,5
6481 à 6599	13	47	60	2,3
6601	-	1	1	2,4
6603 à 6765	18	64	82	2,3
6767	-	1	1	3,4
6769 à 6893	15	48	63	2,3
6895	-	1	1	2,4
6897 à 6927	4	12	16	2,3

6929 à 6931	-	2	2	2,4
6933 à 6963	4	12	16	2,3
6965	-	1	1	2,4
6967 à 6987	4	7	11	2,3
6989	-	1	1	3,4
6991 à 7053	8	24	32	2,3
7055	-	1	1	2,7
7057 à 7105	4	21	25	2,3
7107	-	1	1	2,4
7109 à 7419	31	125	156	2,3
7421	-	1	1	3,4
7423 à 8117	80	268	348	2,3
8119	-	1	1	2,4
8121 à 8337	24	85	109	2,3
8339	-	1	1	2,4
8341 à 8567	22	92	114	2,3
8569	-	1	1	3,4
8571 à 9177	70	234	304	2,3
9179	-	1	1	2,4
9181 à 9501	40	121	161	2,3
9503	-	1	1	3,4
9505 à 9589	7	36	43	2,3
9591	-	1	1	3,4
9593 à 9797	24	79	103	2,3
9799	-	1	1	2,4
9801 à 9807	1	3	4	2,3
9809	-	1	1	2,4
9811 à 9867	8	21	29	2,3
9869	-	1	1	3,4
9871 à 9879	1	4	5	2,3
9881	-	1	1	2,4
9883 à 10401	56	204	260	2,3
10403	-	1	1	2,5
10405 à 10437	3	14	17	2,3
10439	-	1	1	3,4
10441 à 10607	17	67	84	2,3
10609	-	1	1	3,4
10611 à 10761	17	59	76	2,3
10763	-	1	1	2,4
10765 à 10833	5	30	35	2,3
10835	-	1	1	2,4
10837 à 10943	12	42	54	2,3
10945	-	1	1	2,4
10947 à 11039	8	39	47	2,3

11041	-	1	1	3,4
11043 à 11283	27	94	121	2,3
11285	-	1	1	2,4
11287 à 11393	11	43	54	2,3
11395	-	1	1	4,5
11397 à 11659	25	107	132	2,3
11661	-	1	1	2,4
11663 à 11949	32	112	144	2,3
11951	-	1	1	3,4
11953 à 11989	6	13	19	2,3
11991	-	1	1	3,4
11993 à 12119	14	50	64	2,3
12121	-	1	1	3,4
12123 à 13065	101	371	472	2,3
13067	-	1	1	2,4
13069 à 13077	-	5	5	2,3
13079	-	1	1	2,4
13081 à 13131	6	20	26	2,3
13133	-	1	1	3,4
13135 à 13527	38	159	197	2,3
13529	-	1	1	3,4
13531 à 13599	6	29	35	2,3
13601	-	1	1	2,4
13603 à 13733	17	49	66	2,3
13735	-	1	1	3,4
13737 à 13869	12	55	67	2,3
13871	-	1	1	3,4
13873 à 13979	13	41	54	2,3
13981	-	1	1	2,4
13983 à 14025	4	18	22	2,3
14027	-	1	1	2,4
14029 à 14109	9	32	41	2,3
14111	-	1	1	2,4
14113 à 14617	47	206	253	2,3
14619	-	1	1	3,4
14621 à 14699	10	30	40	2,3
14701	-	1	1	3,4
14703 à 14837	18	50	68	2,3
14839	-	1	1	3,5
14841 à 15177	34	135	169	2,3
15179	-	1	1	2,4
15181 à 15503	38	124	162	2,3
15505	-	1	1	3,4
15507 à 15839	37	130	167	2,3

15841	-	1	1	4,8
15843 à 17117	108	530	638	2,3
17119	-	1	1	4,5
17121 à 17167	4	20	24	2,3
17169	-	1	1	3,4
17171 à 17813	66	256	322	2,3
17815	-	1	1	3,4
17817 à 18237	47	164	211	2,3
18239	-	1	1	3,4
18241	-	1	1	2,5
18243 à 18719	47	192	239	2,3
18721	-	1	1	4,6
18723 à 18815	9	38	47	2,3
18817	-	1	1	3,4
18819 à 18999	12	79	91	2,3

Anexo 9.2 – O algoritmo polch1 implementado em FORTRAN 90.

```
program polch1
Use Portlib
implicit none
double precision :: n, a, b, d, e, f, t0, t1, t2, c, q
integer :: i, k, l, j, m, cont,tot=0
integer, dimension(26000) :: v
real(8) tempo
write(*,*)"Teste primalidade de um número positivo ímpar qualquer n"
write(*,*)"Digite dois valores de n ímpares para determinar o intervalo "
tempo = TIMEF()
read*, k
read*, l
     if ( k > 2 )then
     tot=0
    end if
open( unit=8, file = 'chebys.dat', status='unknown' )
         do n = k, l, 2
          open(unit=16,file='result.dat', status='unknown')
          write(16,*)"n=", n
          cont=0
          j = 0
```

```
v = 0
if (n == 0.) then
  t0 = 1.
  c = t0
end if
if (n == 1.) then
  t1 = a
  c = t1
end if
if ( n >= 2. ) then
  do a = 1, n-1
    t0 = 1.
    t1 = a
    do i = 2, n
      b = 2*t1
      d = mod(b,n)
      e = d*a
      f = mod(e,n)
      t2 = f -t0
      c = mod(t2,n)
      t0 = t1
      t1 = c
    end do
```

```
            if ( c < 0 ) then
               c = c + n
            end if
            if ( c /= a ) then
              cont=cont+1
               if ( cont < 3 ) then
                  write(8,*)"Tn(a)/=a para a=", a
               end if
             else
               j = j+1
               v(j) = a
            end if
      end do
      do i = 1, j, 6
         if ( j == n-1 ) then
               write(*,*)'Este n é primo '
         else
              write(16,*)v(i),v(i+1),v(i+2),v(i+3),v(i+4),v(i+5)
         end if

enddo
      if (cont ==0) then
            tot=tot+1
```

```
        end if
 end if

write(8,*)"Para n=", n,"cont=", cont
m=(n-1)-cont
q = (100*m)/n
if ( m /= n-1) then
 write(16,*)"total=",m," % de erro =", q
 write(8,*)" % de erro =", q
end if
end do
write(8,*)"De n=", k, "ate", l,"total de primos", tot
tempo = TIMEF()
write(8,*)"tempo=", tempo
end program polch1
```

Anexo 9.3 – Registros do tempo de execução do algoritmo

Intervalo de n	Tempo em segundos
De n = 1 até 1000	tempo = 825.199999999999900
De n = 1001 até 2000	tempo = 9713.350000000000000
De n = 2001 até 3000	tempo = 14742.770000000000000
De n = 5001 até 6000	tempo = 56232.230000000000000
De n = 8101 até 8500	tempo = 50783.230000000000000
De n = 8501 até 8600	tempo = 12411.180000000000000
De n = 9263 até 9500	tempo = 52199.490000000000000
De n = 10201 até 10300	tempo = 33666.140000000000000
De n = 10301 até 10400	tempo = 35183.740000000000000
De n = 10401 até 10500	tempo = 22207.260000000000000
De n = 10501 até 10600	tempo = 37887.880000000000000
De n = 10655 até 11000	tempo = 109673.640000000000000
De n = 11049 até 11500	tempo = 151700.700000000000000
De n = 11757 até 12000	tempo = 84637.220000000000000
De n = 12099 até 12500	tempo = 171288.940000000000000
De n = 12817 até 13500	tempo = 347150.110000000000000
De n = 13501 até 14000	tempo = 272310.610000000000000
De n =14001 até 14500	tempo = 277879.230000000000000
De n =14501 até 15000	tempo = 307022.580000000000000
De n =15151 até 15500	tempo = 228177.040000000000000
De n = 15965 até 16100	tempo = 124928.640000000000000
De n = 16115 até 16300	tempo = 131652.890000000000000
De n =16353 até 16500	tempo = 84149.050000000000000
De n = 16985 até 17200	tempo = 181861.000000000000000